Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	Related Commands **Command** — **Description** **ip dhcp relay** — Enables or disables the DHCP relay agent. **ip dhcp relay address** — Configures the IP address of a DHCP server on an interface. **ip dhcp relay sub-option type cisco** — Enables DHCP to use Cisco proprietary numbers 150, 152, and 151 when filling the link selection, server ID override, and VRF name/VPN ID relay agent option-82 suboptions. **ip dhcp snooping** — Globally enables DHCP snooping on the device. Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-311.	Related Commands • **ip dhcp snooping** globally enables DHCP snooping. • **ip dhcp snooping vlan** enables DHCP snooping on specified VLANs. • **ip helper-address** enables the DHCP relay agent on a configuration mode interface. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1270.

Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	Examples
	
	This example shows how to enable VRF support for the DHCP relay agent, which is dependent upon enabling Option-82 support for the DHCP relay agent, and how to configure a DHCP server address on a Layer 3 interface when the DHCP server is in a VRF named SiteA:
	
	`switch# configure terminal`
	`switch(config)# ip dhcp relay information option`
	`switch(config)# ip dhcp relay information option vpn`
	`switch(config)# interface ethernet 1/3`
	`switch(config-if)# ip dhcp relay address 10.43.87.132 use-vrf SiteA`
	`switch(config-if)#`
	
	Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-314.
		Example
		• This command enables the attachment of tags to DHCP requests that are forwarded to DHCP server addresses.
		`switch(config)#ip dhcp relay information option`
		`switch(config)#`
		
		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1237.
		
		See also Arista User Manual v. 4.12.3 (7/17/13), at 1068; Arista User Manual, v. 4.11.1 (1/11/13), at 852; Arista User Manual v. 4.10.3 (10/22/12), at 688.

Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	Command — **Description**
	feature dhcp — Enables the DHCP snooping feature on the device.
	ip dhcp relay — Enables the DHCP relay agent.
	ip dhcp relay address — Configures an IP address of a DHCP server on an interface.
	ip dhcp relay information option — Enables the insertion and removal of option-82 information from DHCP packets forwarded by the DHCP relay agent.
	ip dhcp snooping — Globally enables DHCP snooping on the device.
	
	Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-317.
		Example
		• This command enables the DHCP relay agent.
		`switch(config)#ip dhcp relay always-on`
		`switch(config)#`
		
		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1263.
		
		See also Arista User Manual v. 4.12.3 (7/17/13), at 1047; Arista User Manual, v. 4.11.1 (1/11/13), at 890; Arista User Manual v. 4.10.3 (10/22/12), at 688.

Copyright Registration Information	Cisco	Arista

Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	ip dhcp smart-relay
	
	To enable Dynamic Host Configuration Protocol (DHCP) smart relay on a Layer 3 interface, use the **ip dhcp smart-relay** command. To disable DHCP smart relay on a Layer 3 interface, use the **no** form of this command.
	
	ip dhcp smart-relay
	no ip dhcp smart-relay
	
	Syntax Description This command has no arguments or keywords.
	
	Defaults Disabled
	
	Command Modes Interface configuration mode (config-if)
	
	SupportedUserRoles network-admin
	vdc-admin
	
	Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-319.
		ip dhcp smart-relay
		
		The **ip dhcp smart-relay** command configures the DHCP smart relay status on the configuration mode interface. DHCP smart relay supports forwarding DHCP requests with a client's secondary IP addresses in the gateway address field. Enabling DHCP smart relay on an interface requires that DHCP relay is also enabled on that interface.
		
		By default, an interface assumes the global DHCP smart relay setting as configured by the **ip dhcp smart-relay global** command. The **ip dhcp smart-relay** command, when configured, takes precedence over the global smart relay setting.
		
		The **no ip dhcp smart-relay** command disables DHCP smart relay on the configuration mode interface. The **default ip dhcp smart-relay** command restores the interface's to the default DHCP smart relay setting, as configured by the **ip dhcp smart-relay global** command, by removing the corresponding **ip dhcp smart-relay** or **no ip dhcp smart-relay** statement from *running-config*.
		
		Platform all
		Command Mode Interface-Ethernet Configuration
		Interface-Port-channel Configuration
		Interface-VLAN Configuration
		
		Command Syntax
		`ip dhcp smart-relay`
		`no ip dhcp smart-relay`
		`default ip dhcp smart-relay`
		
		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1266.

Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	**Related Commands** **Command** / **Description** **ip dhcp smart-relay** — Enables DHCP smart relay on a Layer 3 interface. **ip dhcp relay** — Enable the DHCP relay agent. Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-322.	Related Commands • ip helper-address enables the DHCP relay agent on a configuration mode interface. • ip dhcp smart-relay enables the DHCP smart relay agent on a configuration mode interface. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1268.

Copyright Registration Information	Cisco	Arista

Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	Examples This example shows how to globally enable DHCP snooping:
	`switch# configure terminal`
	`switch(config)# ip dhcp snooping`
	`switch(config)#`
	
	Related Commands
	Command — **Description**
	feature dhcp — Enables the DHCP snooping feature on the device.
	ip dhcp relay — Enables or disables the DHCP relay agent.
	ip dhcp snooping information option — Enables the insertion and removal of option-82 information for DHCP packets forwarded without the use of the DHCP relay agent.
	ip dhcp snooping trust — Configures an interface as a trusted source of DHCP messages.
	ip dhcp snooping vlan — Enables DHCP snooping on the specified VLANs.
	
	Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-323.
		Command Syntax
		`ip dhcp snooping`
		`no ip dhcp snooping`
		`default ip dhcp snooping`
		
		Related Commands
		• ip dhcp snooping information option enables insertion of option-82 snooping data.
		• ip dhcp snooping vlan enables DHCP snooping on specified VLANs.
		• ip helper-address enables the DHCP relay agent on a configuration mode interface.
		
		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1269.

Copyright Registration Information	Cisco	Arista

Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	ip dhcp snooping information option
	
	To enable the insertion and removal of option-82 information for DHCP packets, use the **ip dhcp snooping information option** command. To disable the insertion and removal of option-82 information, use the **no** form of this command.
	
	ip dhcp snooping information option
	
	no ip dhcp snooping information option
	
	Syntax Description This command has no arguments or keywords.
	
	Defaults By default, the device does not insert and remove option-82 information.
	
	Command Modes Global configuration
	
	SupportedUserRoles network-admin
	vdc-admin
	
	Command History
	| Release | Modification |
	| 4.0(1) | This command was introduced. |
	
	Usage Guidelines To use this command, you must enable the DHCP snooping feature (see the **feature dhcp** command).
	This command does not require a license.
	
	Examples This example shows how to globally enable DHCP snooping:
	`switch# configure terminal`
	`switch(config)# ip dhcp snooping information option`
	`switch(config)#`
	
	Related Commands
	| Command | Description |
	| **ip dhcp relay information option** | Enables the insertion and removal of option-82 information from DHCP packets forwarded by the DHCP relay agent. |
	| **ip dhcp snooping** | Globally enables DHCP snooping on the device. |
	| **ip dhcp snooping trust** | Configures an interface as a trusted source of DHCP messages. |
	| **ip dhcp snooping vlan** | Enables DHCP snooping on the specified VLANs. |
	
	Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-325.
		ip dhcp snooping information option
		
		The **ip dhcp snooping information option** command enables the insertion of option-82 DHCP snooping information in DHCP packets on VLANs where DHCP snooping is enabled. DHCP snooping is a layer 2 switch process that allows relay agents to provide remote-ID and circuit-ID information to DHCP reply and request packets. DHCP servers use this information to determine the originating port of DHCP requests and associate a corresponding IP address to that port.
		
		DHCP snooping uses information option (Option-82) to include the switch MAC address (router-ID) along with the physical interface name and VLAN number (circuit-ID) in DHCP packets. After adding the information to the packet, the DHCP relay agent forwards the packet to the DHCP server through DHCP protocol processes.
		
		VLAN snooping on a specified VLAN requires each of these conditions:
		• DHCP snooping is globally enabled.
		• Insertion of option-82 information in DHCP packets is enabled.
		• DHCP snooping is enabled on the specified VLAN.
		• DHCP relay is enabled on the corresponding VLAN interface.
		
		When global DHCP snooping is not enabled, the **ip dhcp snooping information option** command persists in *running-config* without any operational effect.
		
		The **no ip dhcp snooping information option** and **default ip dhcp snooping information option** commands disable the insertion of option-82 DHCP snooping information in DHCP packets by removing the **ip dhcp snooping information option** statement from *running-config*.
		
		Platform Trident
		Command Mode Global Configuration
		
		Command Syntax
		`ip dhcp snooping information option`
		`no ip dhcp snooping information option`
		`default ip dhcp snooping information option`
		
		Related Commands
		• ip dhcp snooping globally enables DHCP snooping.
		• ip dhcp snooping vlan enables DHCP snooping on specified VLANs.
		• ip helper-address enables the DHCP relay agent on a configuration mode interface.
		
		Example
		• These commands enable DHCP snooping on DHCP packets from ports on snooping-enabled VLANs. DHCP snooping was previously enabled on the switch.
		`switch(config)#ip dhcp snooping information option`
		`switch(config)#show ip dhcp snooping`
		`DHCP Snooping is enabled`
		`DHCP Snooping is operational`
		`DHCP Snooping is configured on following VLANs:`
		`100`
		`DHCP Snooping is operational on following VLANs:`
		`100`
		`Insertion of Option-82 is enabled`
		`Circuit-id format: Interface name:Vlan ID`
		`Remote-id: 00:1c:73:1f:b4:38 (Switch MAC)`
		`switch(config)#`
		
		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1270.

<table>
<tr><th>Copyright Registration Information</th><th>Cisco</th><th>Arista</th></tr>
<tr><td>Cisco NX-OS 6.2

Effective date of registration: 11/13/2014</td><td>
<table>
<tr><th>Related Commands</th><th>Command</th><th>Description</th></tr>
<tr><td></td><td>ip dhcp snooping</td><td>Globally enables DHCP snooping on the device.</td></tr>
<tr><td></td><td>ip dhcp snooping information option</td><td>Enables the insertion and removal of Option-82 information for DHCP packets forwarded without the use of the DHCP relay agent.</td></tr>
<tr><td></td><td>ip dhcp snooping verify mac-address</td><td>Enables MAC address verification as part of DHCP snooping.</td></tr>
<tr><td></td><td>ip dhcp snooping vlan</td><td>Enables DHCP snooping on the specified VLANs.</td></tr>
<tr><td></td><td>show ip dhcp snooping</td><td>Displays general information about DHCP snooping.</td></tr>
<tr><td></td><td>show running-config dhcp</td><td>Displays DHCP snooping configuration, including IP Source Guard configuration.</td></tr>
</table>
Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-328.
</td><td>
ip dhcp snooping vlan

The ip dhcp snooping vlan command enables DHCP snooping on specified VLANs. DHCP snooping is a layer 2 process that allows relay agents to provide remote-ID and circuit-ID information in DHCP packets. DHCP servers use this data to determine the originating port of DHCP requests and associate a corresponding IP address to that port. DHCP snooping is configured on a global and VLAN basis.

Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1271.
</td></tr>
<tr><td>Cisco NX-OS 6.2

Effective date of registration: 11/13/2014</td><td>
<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td>ip dhcp snooping trust</td><td>Configures an interface as a trusted source of DHCP messages.</td></tr>
<tr><td>ip dhcp snooping vlan</td><td>Enables DHCP snooping on the specified VLANs.</td></tr>
<tr><td>show ip dhcp snooping</td><td>Displays general information about DHCP snooping.</td></tr>
<tr><td>show running-config dhcp</td><td>Displays DHCP snooping configuration, including IP Source Guard configuration.</td></tr>
</table>
Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-330.
</td><td>
Related Commands
• ip dhcp snooping globally enables DHCP snooping.
• ip dhcp snooping vlan enables DHCP snooping on specified VLANs.
• ip dhcp snooping information option enables insertion of option-82 snooping data.
• ip helper-address enables the DHCP relay agent on a configuration mode interface.

Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1302.
</td></tr>
</table>

Copyright Registration Information	Cisco	Arista

Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	ip dhcp snooping vlan
	
	To enable DHCP snooping one or more VLANs, use the **ip dhcp snooping vlan** command. To disable DHCP snooping on one or more VLANs, use the **no** form of this command.
	
	ip dhcp snooping vlan *vlan-list*
	
	no ip dhcp snooping vlan *vlan-list*
	
	Syntax Description
	vlan-list — Range of VLANs on which to enable DHCP snooping. The *vlan-list* argument allows you to specify a single VLAN ID, a range of VLAN IDs, or comma-separated IDs and ranges (see the "Examples" section). Valid VLAN IDs are from 1 to 4096.
	
	Defaults
	By default, DHCP snooping is not enabled on any VLAN.
	
	Command Modes
	Global configuration
	
	SupportedUserRoles
	network-admin
	vdc-admin
	
	Command History
	Release: 4.0(1) — Modification: This command was introduced.
	
	Usage Guidelines
	To use this command, you must enable the DHCP snooping feature (see the **feature dhcp** command).
	This command does not require a license.
	
	Examples
	This example shows how to enable DHCP snooping on VLANs 100, 200, and 250 through 252:
	`switch# configure terminal`
	`switch(config)# ip dhcp snooping vlan 100,200,250-252`
	`switch(config)#`
	
	Related Commands
	ip dhcp snooping — Globally enables DHCP snooping on the device.
	ip dhcp snooping information option — Enables the insertion and removal of option-82 information for DHCP packets forwarded without the use of the DHCP relay agent.
	ip dhcp snooping trust — Configures an interface as a trusted source of DHCP messages.
	
	Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-331.
		ip dhcp snooping vlan
		
		The **ip dhcp snooping vlan** command enables DHCP snooping on specified VLANs. DHCP snooping is a layer 2 process that allows relay agents to provide remote-ID and circuit-ID information in DHCP packets. DHCP servers use this data to determine the originating port of DHCP requests and associate a corresponding IP address to that port. DHCP snooping is configured on a global and VLAN basis.
		
		VLAN snooping on a specified VLAN requires each of these conditions:
		• DHCP snooping is globally enabled.
		• Insertion of option-82 information in DHCP packets is enabled.
		• DHCP snooping is enabled on the specified VLAN.
		• DHCP relay is enabled on the corresponding VLAN interface.
		
		When global DHCP snooping is not enabled, the **ip dhcp snooping vlan** command persists in *running-config* without any operational affect.
		
		The **no ip dhcp snooping information option** and **default ip dhcp snooping information option** commands disable DHCP snooping operability by removing the **ip dhcp snooping information option** statement from *running-config*.
		
		Platform: Trident
		Command Mode: Global Configuration
		
		Command Syntax
		`ip dhcp snooping vlan v_range`
		`no ip dhcp snooping vlan v_range`
		`default ip dhcp snooping vlan v_range`
		
		Parameters
		• *v_range* VLANs upon which snooping is enabled. Formats include a number, a number range, or a comma-delimited list of numbers and ranges. Numbers range from 1 to 4094.
		
		Related Commands
		• ip dhcp snooping globally enables DHCP snooping.
		• ip dhcp snooping information option enables insertion of option-82 snooping data.
		• ip helper-address enables the DHCP relay agent on a configuration mode interface.
		
		Example
		• These commands enable DHCP snooping globally, DHCP on VLAN interface100, and DHCP snooping on VLAN 100.
		`switch(config)#ip dhcp snooping`
		`switch(config)#ip dhcp snooping information option`
		`switch(config)#ip dhcp snooping vlan 100`
		`switch(config)#interface vlan 100`
		`switch(config-if-Vl100)#ip helper-address 10.4.4.4`
		`switch(config-if-Vl100)#show ip dhcp snooping`
		`DHCP Snooping is enabled`
		`DHCP Snooping is operational`
		`DHCP Snooping is configured on following VLANs:`
		`100`
		`DHCP Snooping is operational on following VLANs:`
		`100`
		`Insertion of Option-82 is enabled`
		`Circuit-id format: Interface name:Vlan ID`
		`Remote-id: 00:1c:73:1f:b4:38 (Switch MAC)`
		`switch(config)#`
		
		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1302.

Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	**set-dscp-transmit** *dscp-value* — Specifies the differentiated services code point (DSCP) value for IPv4 and IPv6 packets. The range is from 0 to 63. Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-444.	**qos dscp** The qos dscp command specifies the default differentiated services code point (DSCP) value of the configuration mode interface. The default DSCP determines the traffic class for non-IP packets that are inbound on DSCP trusted ports. DSCP trusted ports determine the traffic class for inbound packets as follows: Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1093. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 991; Arista User Manual, v. 4.11.1 (1/11/13), at 795; Arista User Manual v. 4.10.3 (10/22/12), at 646; Arista User Manual v. 4.9.3.2 (5/3/12), at 576; Arista User Manual v. 4.8.2 (11/18/11), at 666.

Copyright Registration Information	Cisco	Arista

Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	policy-map type control-plane
	
	To create or specify a control plane policy map and enter policy map configuration mode, use the **policy-map type control-plane** command. To delete a control plane policy map, use the **no** form of this command.
	
	policy-map type control-plane *policy-map-name*
	
	no policy-map type control-plane *policy-map-name*
	
	Syntax Description — *policy-map-name*: Name of the class map. The name is alphanumeric, case sensitive, and has a maximum of 64 characters.
	
	Defaults — None
	
	Command Modes — Global configuration
	
	SupportedUserRoles — network-admin, vdc-admin
	
	Command History
	Release: 4.0(1) — Modification: This command was introduced.
	
	Usage Guidelines — You can use this command only in the default VDC.
	This command does not require a license.
	
	Examples — This example shows how to specify a control plane policy map and enter policy map configuration mode:
	`switch# config t`
	`switch(config)# policy-map type control-plane PolicyMapA`
	`switch(config-pmap)#`
	
	This example shows how to delete a control plane policy map:
	`switch# config t`
	`switch(config)# no policy-map type control-plane PolicyMapA`
	
	Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-448.
		policy-map type control-plane
		
		The **policy-map type control-plane** command places the switch in Policy-Map (control plane) configuration mode, which is a group change mode that modifies a control-plane policy map. A policy map is a data structure that consists of class maps that identify a specific data stream and specify bandwidth and shaping parameters that controls its transmission. Control plane policy maps are applied to the control plane to manage traffic.
		
		The **copp-system-policy** policy map is supplied with the switch and is always applied to the control plane. **Copp-system-policy** is the only valid control plane policy map.
		
		The **exit** command saves pending policy map changes to *running-config* and returns the switch to global configuration mode. Policy map changes are also saved by entering a different configuration mode. The **abort** command discards pending changes, returning the switch to global configuration mode.
		
		The **no policy-map type control-plane** and **default policy-map type control-plane** commands delete the specified policy map by removing the corresponding **policy-map type control-plane** command and its associated configuration.
		
		Platform: FM6000, Petra, Trident
		Command Mode: Global Configuration
		
		Command Syntax
		`policy-map type control-plane copp-system-policy`
		`no policy-map type control-plane copp-system-policy`
		`default policy-map type control-plane copp-system-policy`
		
		copp-system-policy is supplied with the switch and is the only valid control plane policy map.
		
		Commands Available in Policy-Map Configuration Mode
		• class (policy-map (control-plane) – FM6000)
		• class (policy-map (control-plane) – Trident)
		
		Related Commands
		• class-map type control-plane enters control-plane class-map configuration mode.
		
		Example
		• This command places the switch in policy-map configuration mode to edit the copp-system-policy policy map.
		`switch(config)#policy-map type control-plane copp-system-policy`
		`switch(config-pmap-copp-system-policy)#`
		
		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1194.
		
		See also Arista User Manual v. 4.12.3 (7/17/13), at 980; Arista User Manual, v. 4.11.1 (1/11/13), at 784.

Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	To view per-entry statistics, use the **show access-lists** command or the applicable following command: • **show ip access-lists** • **show ipv6 access-lists** • **show mac access-lists** Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-517.	**Displaying Contents of an ACL** These commands display ACL contents. • show ip access-lists • show ipv6 access-lists • show mac access-lists Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 845. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 724; Arista User Manual, v. 4.11.1 (1/11/13), at 552; Arista User Manual v. 4.10.3 (10/22/12), at 466.

Copyright Registration Information	Cisco	Arista

Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	Examples This example shows how to display control plane class map information:
	`switch# show class-map type control-plane`
	
	`class-map type control-plane match-any copp-system-class-critical`
	`  match access-grp name copp-system-acl-arp`
	`  match access-grp name copp-system-acl-msdp`
	
	`class-map type control-plane match-any copp-system-class-important`
	`  match access-grp name copp-system-acl-gre`
	`  match access-grp name copp-system-acl-tacas`
	
	`class-map type control-plane match-any copp-system-class-normal`
	`  match access-grp name copp-system-acl-icmp`
	`  match redirect dhcp-snoop`
	`  match redirect arp-inspect`
	`  match exception ip option`
	`  match exception ip icmp redirect`
	`  match exception ip icmp unreachable`
	
	Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-552.
		Example
		• This command displays all control plane class maps.
		• This command displays the available control plane class maps.
		`switch>show class-map type control-plane`
		`  Class-map: CM-CP1 (match-any)`
		`  Match: ip access-group name LIST-CP1`
		`  Class-map: copp-system-acllog (match-any)`
		`  Class-map: copp-system-arp (match-any)`
		`  Class-map: copp-system-arpresolver (match-any)`
		`  Class-map: copp-system-bpdu (match-any)`
		`  Class-map: copp-system-glean (match-any)`
		`  Class-map: copp-system-igmp (match-any)`
		`  Class-map: copp-system-ipmcmiss (match-any)`
		`  Class-map: copp-system-ipmcrsvd (match-any)`
		`  Class-map: copp-system-l3destmiss (match-any)`
		`  Class-map: copp-system-l3slowpath (match-any)`
		`  Class-map: copp-system-l3ttl1 (match-any)`
		`  Class-map: copp-system-lacp (match-any)`
		`  Class-map: copp-system-lldp (match-any)`
		`  Class-map: copp-system-selfip (match-any)`
		`  Class-map: copp-system-selfip-tc6to7 (match-any)`
		`  Class-map: copp-system-sflow (match-any)`
		`  Class-map: copp-system-tc3to5 (match-any)`
		`  Class-map: copp-system-tc6to7 (match-any)`
		`switch>`
		
		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/20140), at 1212.

Copyright Registration Information	Cisco	Arista

Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	Examples
	This example shows how to display the DHCP relay status and configured DHCP server addresses:
	`switch# show ip dhcp relay`
	`DHCP relay service is enabled`
	`Insertion of option 82 is enabled`
	`Insertion of VPN suboptions is enabled`
	`Helper addresses are configured on the following interfaces:`
	`Interface Relay Address VRF Name`
	`Ethernet1/4 10.10.10.1 red`
	`switch#`
	
	Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-630.
		Example
		• This command displays the DHCP relay agent configuration status.
		`switch>show ip dhcp relay`
		`DHCP servers: 172.22.22.11`
		`Vlan1000:`
		`DHCP clients are permitted on this interface`
		
		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1237.
		
		See also Arista User Manual v. 4.12.3 (7/17/13), at 1047; Arista User Manual, v. 4.11.1 (1/11/13), at 868; Arista User Manual v. 4.10.3 (10/22/12), at 716.

Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	Examples
	This example shows how to display general status information about DHCP snooping:
	`switch# show ip dhcp snooping`
	`DHCP snooping service is enabled`
	`Switch DHCP snooping is enabled`
	`DHCP snooping is configured on the following VLANs:`
	`1,13`
	`DHCP snooping is operational on the following VLANs:`
	`1`
	`Insertion of Option 82 is disabled`
	`Verification of MAC address is enabled`
	`DHCP snooping trust is configured on the following interfaces:`
	`Interface Trusted`
	`Ethernet2/3 Yes`
	`switch#`
	
	Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-634.
		Example
		• This command DHCP snooping hardware status.
		`switch>show ip dhcp snooping hardware`
		`DHCP Snooping is enabled`
		`DHCP Snooping is enabled on following VLANs:`
		`None`
		`Vlans enabled per Slice`
		`Slice: FixedSystem`
		`None`
		`switch>`
		
		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1304.

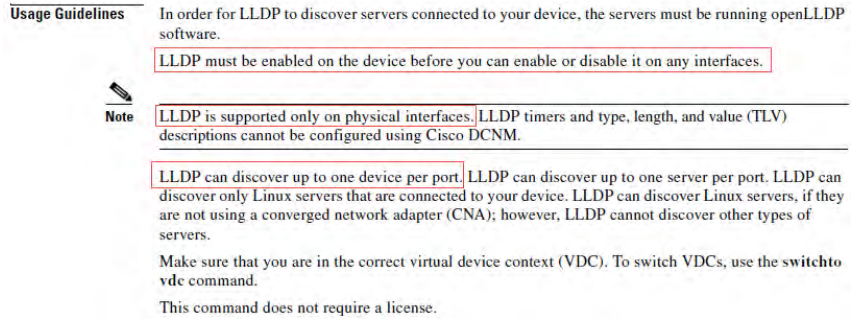
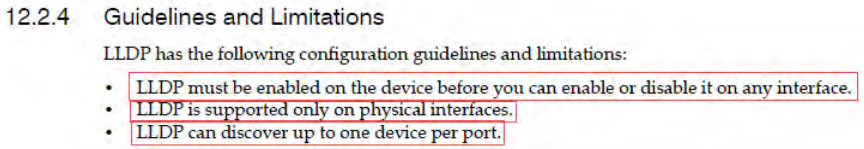
Copyright Registration Information	Cisco	Arista

Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	Examples
	This example shows how to use the **show port-security** command to view the status of the port security feature on a device:
	`switch# show port-security`
	`Total Secured Mac Addresses in System (excluding one mac per port) : 0`
	`Max Addresses limit in System (excluding one mac per port) : 8192`
	
	Secure Port | MaxSecureAddr (Count) | CurrentAddr (Count) | SecurityViolation (Count) | Security Action
	Ethernet1/4 | 5 | 1 | 0 | Shutdown
	`switch#`
	
	Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-661.
		Example
		• These commands enable MAC security on Ethernet interface 7, set the maximum number of assigned MAC addresses to 2, assigns two static MAC addresses to the interface, and clears the dynamic MAC addresses for the interface.
		`switch(config)#interface ethernet 7`
		`switch(config-if-Et7)#switchport port-security`
		`switch(config-if-Et7)#switchport port-security maximum 2`
		`switch(config-if-Et7)#exit`
		`switch(config)#mac address-table static 0034.24c2.8f11 vlan 10 interface ethernet 7`
		`switch(config)#mac address-table static 4464.842d.17ce vlan 10 interface ethernet 7`
		`switch(config)#clear mac address-table dynamic interface ethernet 7`
		`switch(config)#show port-security`
		Secure Port | MaxSecureAddr (Count) | CurrentAddr (Count) | SecurityViolation (Count) | Security Action
		Et7 | 2 | 2 | 0 | Shutdown
		`Total Addresses in System: 1`
		`switch(config)#show port-security address`
		Secure Mac Address Table
		Vlan | Mac Address | Type | Ports | Remaining Age (mins)
		10 | 0034.24c2.8f11 | SecureConfigured | Et7 | N/A
		10 | 4464.842d.17ce | SecureConfigured | Et7 | N/A
		`Total Mac Addresses for this criterion: 2`
		`switch(config)#`
		
		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 632.
		
		See also Arista User Manual v. 4.13.6F (4/14/2014), at 624; Arista User Manual v. 4.12.3 (7/17/13), at 501; Arista User Manual, v. 4.11.1 (1/11/13), at 405-06; Arista User Manual v. 4.10.3 (10/22/12), at 336; Arista User Manual v. 4.9.3.2 (5/3/12), at 405-06.

Copyright Registration Information	Cisco	Arista

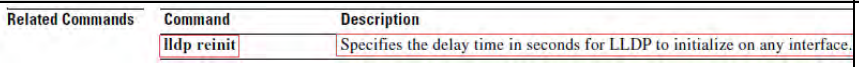
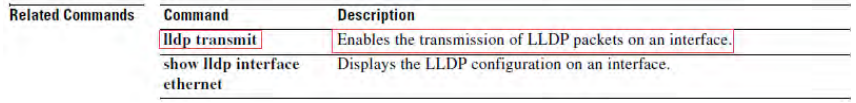
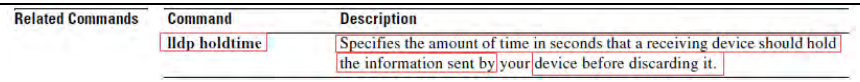
Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	Examples
	This example shows how to use the **show port-security address** command to view information about all MAC addresses secured by port security:
	`switch# show port-security address`
	`Total Secured Mac Addresses in System (excluding one mac per port) : 0`
	`Max Addresses limit in System (excluding one mac per port) : 8192`
	Secure Mac Address Table
	Vlan / Mac Address / Type / Ports / Remaining Age (mins)
	1 0054.AAB3.770F STATIC port-channel1 0
	1 00EE.378A.ABCE STATIC Ethernet1/4 0
	`switch#`
	This example shows how to use the **show port-security address** command to view the MAC addresses secured by the port security feature on the Ethernet 1/4 interface:
	`switch# show port-security address interface ethernet 1/4`
	Secure Mac Address Table
	Vlan / Mac Address / Type / Ports / Remaining Age (mins)
	1 00EE.378A.ABCE STATIC Ethernet1/4 0
	`switch#`
	
	Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-664.
		Example
		• This command displays MAC addresses assigned to port-security protected interfaces.
		`switch>show port-security address`
		Secure Mac Address Table
		Vlan / Mac Address / Type / Ports / Remaining Age (mins)
		10 164f.29ae.4e14 SecureConfigured Et7 N/A
		10 164f.29ae.4f11 SecureConfigured Et7 N/A
		10 164f.320a.3a11 SecureConfigured Et7 N/A
		`Total Mac Addresses for this criterion: 3`
		`switch>`
		
		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 698.
		
		See also Arista User Manual v. 4.12.3 (7/17/13), at 562; Arista User Manual, v. 4.11.1 (1/11/13), at 446; Arista User Manual v. 4.10.3 (10/22/12), at 366; Arista User Manual v. 4.9.3.2 (5/3/12), at 338.

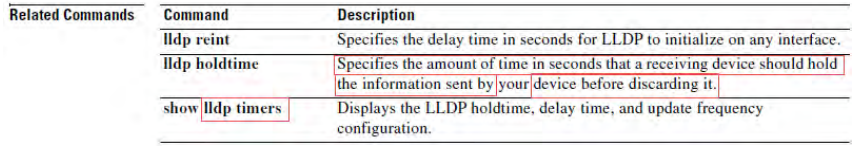
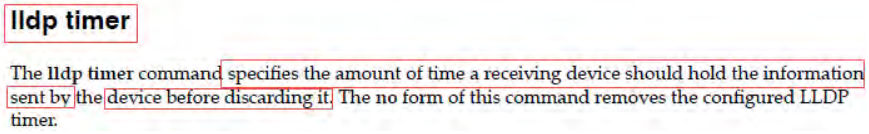
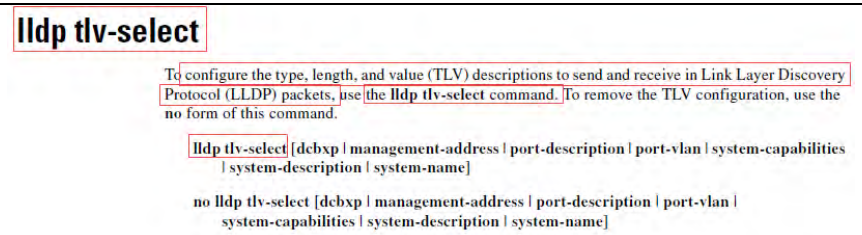
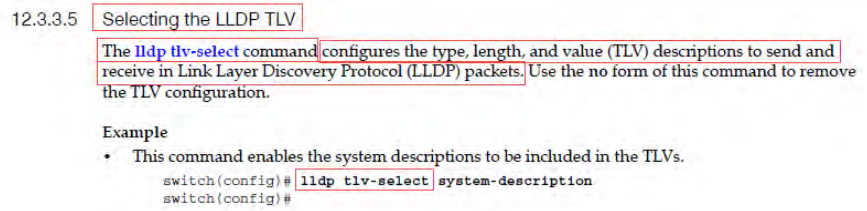
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	**Related Commands** **Command** / **Description** **feature dhcp** — Enables the DHCP snooping feature on the device. **ip dhcp snooping** — Globally enables DHCP snooping on the device. **service dhcp** — Enables or disables the DHCP relay agent. **show ip dhcp snooping** — Displays general information about DHCP snooping. **show ip dhcp snooping binding** — Displays IP-MAC address bindings, including the static IP source entries. Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-695.	**ip dhcp snooping** The **ip dhcp snooping** command enables DHCP snooping globally on the switch. DHCP snooping is a set of layer 2 processes that can be configured on LAN switches and used with DHCP servers to control network access to clients with specific IP/MAC addresses. The swtich supports Option-82 insertion, which is a DHCP snooping process that allows relay agents to provide remote-ID and circuit-ID information to DHCP reply and request packets. DHCP servers use this information to determine the originating port of DHCP requests and associate a corresponding IP address to that port. DHCP servers use port information to track host location and IP address usage by authorized physical ports. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1269.

Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 **Usage Guidelines** In order for LLDP to discover servers connected to your device, the servers must be running openLLDP software. LLDP must be enabled on the device before you can enable or disable it on any interfaces. **Note** LLDP is supported only on physical interfaces. LLDP timers and type, length, and value (TLV) descriptions cannot be configured using Cisco DCNM. LLDP can discover up to one device per port. LLDP can discover up to one server per port. LLDP can discover only Linux servers that are connected to your device. LLDP can discover Linux servers, if they are not using a converged network adapter (CNA); however, LLDP cannot discover other types of servers. Make sure that you are in the correct virtual device context (VDC). To switch VDCs, use the **switchto vdc** command. This command does not require a license. Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 174.	 12.2.4 Guidelines and Limitations LLDP has the following configuration guidelines and limitations: • LLDP must be enabled on the device before you can enable or disable it on any interface. • LLDP is supported only on physical interfaces. • LLDP can discover up to one device per port. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 576. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 448; Arista User Manual, v. 4.11.1 (1/11/13), at 366.

Copyright Registration Information	Cisco	Arista

Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	lldp holdtime
	
	To configure the amount of time that a receiving device should hold the information sent by your device before discarding it, use the **lldp holdtime** command. To remove the hold time configuration, use the **no** form of this command.
	
	lldp holdtime *seconds*
	
	Syntax Description *seconds* Hold time in seconds. The range is from 10 to 255 seconds.
	
	Defaults 120 seconds
	
	Command Modes Global configuration mode (config)
	
	SupportedUserRoles network-admin
	network-operator
	vdc-admin
	vdc-operator
	
	Command History
	Release **Modification**
	5.0(1) This command was introduced.
	
	Usage Guidelines Make sure that you are in the correct virtual device context (VDC). To switch VDCs, use the **switchto vdc** command.
	This command does not require a license.
	
	Examples This example shows how to configure the Link Layer Discovery Protocol (LLDP) hold time:
	`switch(config)# lldp holdtime 180`
	`switch(config)#`
	
	This example shows how to remove the LLDP hold time configuration:
	`switch(config)# no lldp holdtime 180`
	`switch(config)#`
	
	Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 228.
		lldp holdtime
		
		The **lldp holdtime** command specifies the amount of time a receiving device should hold the information sent by the device before discarding it.
		
		Platform all
		Command Mode Global Configuration
		
		Command Syntax
		`lldp holdtime` *period*
		`no lldp holdtime`
		`default lldp holdtime`
		
		Parameters
		• *period* The amount of time a receiving device should hold the LLDPDU information sent before discarding it. Value ranges from 10 to 65535 second; default value is 120 seconds.
		
		Examples
		• This command sets the amount of time to 180 seconds before the receiving device discards the LLDPDU information.
		`switch(config)# lldp holdtime 180`
		`switch(config)#`
		• This command removes the configured time before the receiving device discards the LLDPDU information.
		`switch(config)# no lldp holdtime 180`
		`switch(config)#`
		
		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 585.
		
		See also Arista User Manual v. 4.12.3 (7/17/13), at 458; Arista User Manual, v. 4.11.1 (1/11/13), at 376.

Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 Related Commands / Command / Description lldp reinit — Specifies the delay time in seconds for LLDP to initialize on any interface. Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 228.	**lldp reinit** The **lldp reinit** command specifies the delay time in seconds for LLDP to initialize on any interface. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 589. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 462; Arista User Manual, v. 4.11.1 (1/11/13), at 380.
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 Related Commands / Command / Description lldp transmit — Enables the transmission of LLDP packets on an interface. show lldp interface ethernet — Displays the LLDP configuration on an interface. Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 231.	**lldp transmit** The **lldp transmit** command enables the transmission of LLDP packets on an interface. After you globally enable LLDP, it is enabled on all supported interfaces by default. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 593. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 446; Arista User Manual, v. 4.11.1 (1/11/13), at 384.
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 Related Commands / Command / Description lldp holdtime — Specifies the amount of time in seconds that a receiving device should hold the information sent by your device before discarding it. Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 232.	12.3.3.2 Setting the LLDP Hold Time The **lldp holdtime** command specifies the amount of time in seconds that a receiving device should hold the information sent by the device before discarding it. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 578. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 450; Arista User Manual, v. 4.11.1 (1/11/13), at 368.

Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 Related Commands Command — Description lldp reint — Specifies the delay time in seconds for LLDP to initialize on any interface. lldp holdtime — Specifies the amount of time in seconds that a receiving device should hold the information sent by your device before discarding it. show lldp timers — Displays the LLDP holdtime, delay time, and update frequency configuration. Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 235.	 lldp timer The lldp timer command specifies the amount of time a receiving device should hold the information sent by the device before discarding it. The no form of this command removes the configured LLDP timer. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 591. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 464; Arista User Manual, v. 4.11.1 (1/11/13), at 382.
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 lldp tlv-select To configure the type, length, and value (TLV) descriptions to send and receive in Link Layer Discovery Protocol (LLDP) packets, use the lldp tlv-select command. To remove the TLV configuration, use the no form of this command. lldp tlv-select [dcbxp | management-address | port-description | port-vlan | system-capabilities | system-description | system-name] no lldp tlv-select [dcbxp | management-address | port-description | port-vlan | system-capabilities | system-description | system-name] Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 236.	 12.3.3.5 Selecting the LLDP TLV The lldp tlv-select command configures the type, length, and value (TLV) descriptions to send and receive in Link Layer Discovery Protocol (LLDP) packets. Use the no form of this command to remove the TLV configuration. Example • This command enables the system descriptions to be included in the TLVs. switch(config)# lldp tlv-select system-description switch(config)# Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 578. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 465; Arista User Manual, v. 4.11.1 (1/11/13), at 368-69.

Copyright Registration Information	Cisco	Arista

Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	logging console
	
	To enable logging messages to the console session, use the **logging console** command. To disable logging messages to the console session, use the **no** form of this command.
	
	logging console [*severity-level*]
	
	no logging console
	
	Syntax Description
	severity-level (Optional) Number of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows:
	• **0**—emergency: System unusable
	• **1**—alert: Immediate action needed
	• **2**—critical: Critical condition—default level
	• **3**—error: Error condition
	• **4**—warning: Warning condition
	• **5**—notification: Normal but significant condition
	• **6**—informational: Informational message only
	• **7**—debugging: Appears during debugging only
	
	Defaults
	None
	
	Command Modes
	Global configuration mode
	
	SupportedUserRoles
	network-admin
	vdc-admin
	
	Command History
	Release: 4.0(1) — Modification: This command was introduced.
	
	Usage Guidelines
	This command does not require a license.
	
	Examples
	This example shows how to enable logging messages with a severity level of 4 (warning) or higher to the console session:
	`switch# configure terminal`
	`switch(config)# logging console 4`
	`switch(config)#`
	
	Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 242.
		logging trap system
		
		The **logging trap system** command enables the logging of system messages to a remote server, or limits the syslog messages saved to a remote server based on severity. Use this command without a specified level to enable remote logging.
		
		The **no logging trap system** and **default logging trap system** commands clear the specified method list by removing the corresponding **logging trap system** command from *running-config*.
		
		Platform: all
		Command Mode: Global Configuration
		
		Command Syntax
		`logging trap system [FACILITY_LEVEL] [CONDITION] [PROGRAM] [TEXT]`
		`no logging trap system [FACILITY_LEVEL] [CONDITION] [PROGRAM] [TEXT]`
		`default logging trap system [FACILITY_LEVEL] [CONDITION] [PROGRAM] [TEXT]`
		
		The *TEXT* parameter, when present, is always last. All other parameters can be placed in any order.
		
		Parameters
		• *FACILITY_LEVEL* Defines the appropriate facility.
		— <no parameter> Specifies default facility.
		— **facility** <*facility-name*> Specifies named facility.
		• *CONDITION* Specifies condition level. Options include:
		— <no parameter> Specifies default condition level.
		— **severity** <*condition-level*> Name of the severity level at which messages should be logged.
		Valid *condition-level* options include:
		❄ **0 or emergencies** System is unusable
		❄ **1 or alerts** Immediate action needed
		❄ **2 or critical** Critical conditions
		❄ **3 or errors** Error conditions
		❄ **4 or warnings** Warning conditions
		❄ **5 or notifications** Normal but significant conditions
		❄ **6 or informational** Informational messages
		❄ **7 or debugging** Debugging messages
		• *PROGRAM* Filters packets based on program name. Options include:
		— <no parameter> All tags or program names.
		— **tag** *program-name* Specific tag or program name.
		• *TEXT* Specifies log message text. Options include:
		— <no parameter> Specify text contained in log message.
		— **contain** *reg-expression* Specify text contained in log message.
		
		Examples
		• This command enables the logging of system informational messages to a remote server.
		`switch(config)#logging trap informational`
		`switch(config)#`
		
		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2015), at 155.

Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	To configure the interval between Precision Time Protocol (PTP) announce messages on an interface or the number of PTP intervals before a timeout occurs on an interface, use the **ptp announce** command. To remove the interval configuration for PTP messages, use the **no** form of this command. Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 330.	**Set the Peer Delay Request Interval** To configure the minimum interval allowed between Precision Time Protocol (PTP) peer delay-request messages, use the **ptp pdelay-req interval** command. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 273. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 216.

Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	Examples
	This example shows how to configure the interval between PTP announce messages on an interface:
	`switch# configure terminal`
	`switch(config)# interface ethernet 5/1`
	`switch(config-if)# ptp announce interval 1`
	`switch(config-if)#`
	
	Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 330.
		Examples
		• This command shows how to configure the interval between PTP announce messages on an interface.
		`switch(config)# interface ethernet 5`
		`switch(config-if-Et5)# ptp announce interval 1`
		`switch(config-if-Et5)#`
		
		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 315.
		
		See also Arista User Manual v. 4.12.3 (7/17/13), at 253; Arista User Manual, v. 4.11.1 (1/11/13), at 199.

Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	**Related Commands** **Command** — **Description** **ptp** — Enables or disables PTP on an interface. **ptp announce** — Configures the interval between PTP announce messages on an interface or the number of PTP intervals before a timeout occurs on an interface. **ptp sync interval** — Configures the interval between PTP synchronization messages on an interface. **ptp vlan vlan** — Configures the PTP VLAN value on an interface. Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 333.	**ptp announce interval** The ptp announce interval command configures the interval between PTP announcement messages on or the number of PTP intervals before a timeout occurs. To disable this feature, use the no form of this command. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 315. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 253; Arista User Manual, v. 4.11.1 (1/11/13), at 199.

Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	**ptp delay-request minimum interval** To configure the minimum interval allowed between Precision Time Protocol (PTP) delay-request messages when the port is in the master state, use the **ptp delay-request minimum interval** command. To remove the minimum interval configuration for PTP delay-request messages, use the **no** form of this command. Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 332.	**ptp delay-req interval** The **ptp delay-req interval** command specifies the time recommended to the slave devices to send delay request messages. You must enable PTP on the switch first and configure the source IP address for PTP communication. To remove the minimum interval configuration for PTP delay-request messages, use the no form of this command. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 318. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 256; Arista User Manual, v. 4.11.1 (1/11/13), at 202.
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	Related Commands **Command** / **Description** **feature ptp** — Enables or disables PTP on the device. **ptp source** — Configures the source IP address for all PTP packets. **ptp priority1** — Configures the priority1 value to use when advertising this clock. **ptp priority2** — Configures the priority2 value to use when advertising this clock. Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 334.	**ptp source ip** The **ptp source ip** command configures the source IP address for all PTP packets. The IP address can be in IPv4 format. To remove PTP settings, use the no form of this command. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 328. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 264; Arista User Manual, v. 4.11.1 (1/11/13), at 210.

Copyright Registration Information	Cisco	Arista

Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	ptp priority1
	
	To configure the priority1 value when advertising the Precision Time Protocol (PTP) clock, use the **ptp priority1** command. To remove the priority1 value, use the **no** form of this command.
	
	ptp priority1 *priority-number*
	
	no ptp priority1 *priority-number*
	
	Syntax Description *priority-number* Priority number. The range is from 0 to 255.
	
	Defaults 255
	
	Command Modes Global configuration mode (config)
	
	SupportedUserRoles network-admin
	vdc-admin
	
	Command History
	Release **Modification**
	5.2(1) This command was introduced.
	
	Usage Guidelines This command does not require a license.
	
	Examples This example shows how to configure the priority1 value when advertising the PTP clock:
	`switch# configure terminal`
	`switch(config)# ptp priority1 10`
	
	This example shows how to remove the priority1 value when advertising the PTP clock:
	`switch# configure terminal`
	`switch(config)# no ptp priority1 10`
	
	Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 336.
		Set the PTP Priority1
		
		To configure the priority1 value when advertising the clock, use the ptp priority1 command. This value overrides the default criteria for best master clock selection. Lower values take precedence.
		
		• The ptp priority1 command configures the priority1 value of 120 to use when advertising the clock.
		`switch(config)# ptp priority1 120`
		`switch(config)#`
		
		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 272.
		
		See also Arista User Manual v. 4.12.3 (7/17/13), at 214-15.

Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	**Related Commands** **Command** / **Description** **feature ptp** — Enables or disables PTP on the device. **ptp source** — Configures the source IP address for all PTP packets. **ptp domain** — Configures the domain number to use for this clock. **ptp priority2** — Configures the priority2 value to use when advertising this clock. **show ptp brief** — Displays the PTP status. **show ptp clock** — Displays the properties of the local clock. Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 336.	**ptp domain** The ptp domain command configures the domain number to use for the clock. PTP domains allow you to use multiple independent PTP clocking subdomains on a single network. To remove PTP settings, use the no form of this command. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 319. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 257; Arista User Manual, v. 4.11.1 (1/11/13), at 204.

Copyright Registration Information	Cisco	Arista

Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	ptp priority2
	
	To configure the priority2 value when advertising the Precision Time Protocol (PTP) clock, use the **ptp priority2** command. To remove the priority2 value when advertising the PTP, use the **no** form of this command.
	
	ptp priority2 *priority-number*
	
	no ptp priority2 *priority-number*
	
	Syntax Description — *priority-number*: Priority number. The range is from 0 to 255.
	
	Defaults: 255
	
	Command Modes: Global configuration mode (config)
	
	SupportedUserRoles: network-admin
	vdc-admin
	
	Command History
	Release: 5.2(1) — Modification: This command was introduced.
	
	Usage Guidelines: This command does not require a license.
	
	Examples: This example shows how to configure the priority2 value when advertising the PTP clock:
	`switch# configure terminal`
	`switch(config)# ptp priority2 1`
	
	This example shows how to remove the priority2 value configuration for use when advertising the PTP clock:
	`switch# configure terminal`
	`switch(config)# no ptp priority2 1`
	
	Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 337.
		Set the PTP Priority2
		
		To configure the priority2 value when advertising this clock, use the ptp priority2 command. This value is used to decide between two devices that are otherwise equally matched in the default criteria.
		
		• The ptp priority2 command configures the priority2 value of 128 to use when advertising this clock.
		`switch(config)# ptp priority2 128`
		`switch(config)#`
		
		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 272.
		
		See also Arista User Manual v. 4.12.3 (7/17/13), at 215.

Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	Related Commands **Command** — **Description** feature ptp — Enables or disables PTP on the device. ptp source — Configures the source IP address for all PTP packets. ptp domain — Configures the domain number to use for this clock. ptp priority1 — Configures the priority1 value to use when advertising this clock. Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 337.	**ptp source ip** The ptp source ip command configures the source IP address for all PTP packets. The IP address can be in IPv4 format. To remove PTP settings, use the no form of this command. Arista User Manual v. 4.14.3F – Rev. 2 10/2/2014), at 328. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 264; Arista User Manual, v. 4.11.1 (1/11/13), at 210.
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	Related Commands **Command** — **Description** feature ptp — Enables or disables PTP on the device. ptp source — Configures the source IP address for all PTP packets. ptp domain — Configures the domain number to use for this clock. ptp priority1 — Configures the priority1 value to use when advertising this clock. Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 337.	**ptp domain** The ptp domain command configures the domain number to use for the clock. PTP domains allow you to use multiple independent PTP clocking subdomains on a single network. To remove PTP settings, use the no form of this command. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 319. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 257; Arista User Manual, v. 4.11.1 (1/11/13), at 204.

Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	Command — **Description**
	ptp priority1 — Configures the priority1 value to use when advertising this clock.
	ptp priority2 — Configures the priority2 value to use when advertising this clock.
	show ptp brief — Displays the PTP status.
	show ptp clock — Displays the properties of the local clock.
	
	Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 340.
		Set the PTP Priority1
		
		To configure the priority1 value when advertising the clock, use the ptp priority1 command. This value overrides the default criteria for best master clock selection. Lower values take precedence.
		• The ptp priority1 command configures the priority1 value of 120 to use when advertising the clock.
		`switch(config)# ptp priority1 120`
		`switch(config)#`
		
		Set the PTP Prioriity2
		
		To configure the priority2 value when advertising this clock, use the ptp priority2 command. This value is used to decide between two devices that are otherwise equally matched in the default criteria.
		• The ptp priority2 command configures the priority2 value of 128 to use when advertising this clock.
		`switch(config)# ptp priority2 128`
		`switch(config)#`
		
		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 272.
		
		See also Arista User Manual v. 4.12.3 (7/17/13), at 214-15.

Copyright Registration Information	Cisco	Arista

Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	ptp sync interval
	
	To configure the interval between Precision Time Protocol (PTP) synchronization messages on an interface, use the **ptp sync interval** command. To remove the interval configuration for PTP messages synchronization, use the **no** form of this command.
	
	ptp sync interval *seconds*
	
	no ptp sync interval *seconds*
	
	Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 340.
		Set the Peer Delay Request Interval
		
		To configure the minimum interval allowed between Precision Time Protocol (PTP) peer delay-request messages, use the **ptp pdelay-req interval** command.
		
		• The **ptp pdelay-req interval** command configures the minimum interval allowed between Precision Time Protocol (PTP) peer delay-request messages to 3.
		
		`switch(config-if-Et5)# ptp pdelay-request interval 3`
		`switch(config-if-Et5)#`
		
		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 273.
		
		See also Arista User Manual v. 4.12.3 (7/17/13), at 216.

Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	ptp sync interval
	
	To configure the interval between Precision Time Protocol (PTP) synchronization messages on an interface, use the **ptp sync interval** command. To remove the interval configuration for PTP messages synchronization, use the **no** form of this command.
	
	ptp sync interval *seconds*
	
	no ptp sync interval *seconds*
	
	Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 340.
		ptp delay-req interval
		
		The **ptp delay-req interval** command specifies the time recommended to the slave devices to send delay request messages. You must enable PTP on the switch first and configure the source IP address for PTP communication. To remove the minimum interval configuration for PTP delay-request messages, use the no form of this command.
		
		Platform Arad, FM6000
		Command Mode Interface-Ethernet Configuration
		Interface-Port Channel Configuration
		
		Command Syntax
		`ptp delay-req interval log_interval`
		`no ptp delay-req interval`
		`default ptp delay-req interval`
		
		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 318.
		
		See also Arista User Manual v. 4.12.3 (7/17/13), at 256; Arista User Manual, v. 4.11.1 (1/11/13), at 202.

Copyright Registration Information	Cisco	Arista

Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	Related Commands
	
	Command / **Description**
	ptp — Enables or disables PTP on an interface.
	ptp announce — Configures the interval between PTP announce messages on an interface or the number of PTP intervals before a timeout occurs on an interface.
	ptp delay-request minimum interval — Configures the minimum interval allowed between PTP delay-request messages when the port is in the master state.
	ptp vlan vlan — Configures the PTP VLAN value on an interface.
	
	Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 342.
		Examples
		• This command shows how to configure the minimum interval allowed between PTP delay-request messages.
		`switch(config)# interface ethernet 5`
		`switch(config-if-Et5)# ptp delay-request interval 3`
		`switch(config-if-Et5)#`
		• This command removes the configured minimum interval allowed between PTP delay-request messages.
		`switch(config)# interface ethernet 5`
		`switch(config-if-Et5)# no ptp delay-request interval`
		`switch(config-if-Et5)#`
		
		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 318.
		
		See also Arista User Manual v. 4.12.3 (7/17/13), at 256; Arista User Manual, v. 4.11.1 (1/11/13), at 202.

Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	Make sure that you have globally enabled PTP on the device and configured the source IP address for PTP communication. Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 343.	The **ptp delay-req interval** command specifies the time recommended to the slave devices to send delay request messages. You must enable PTP on the switch first and configure the source IP address for PTP communication. To remove the minimum interval configuration for PTP delay-request messages, use the no form of this command. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 318. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 256; Arista User Manual, v. 4.11.1 (1/11/13), at 202.

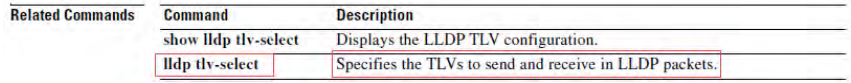
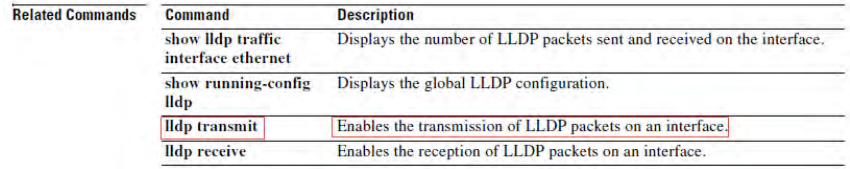
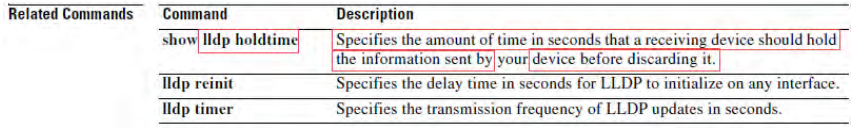
Copyright Registration Information	Cisco	Arista

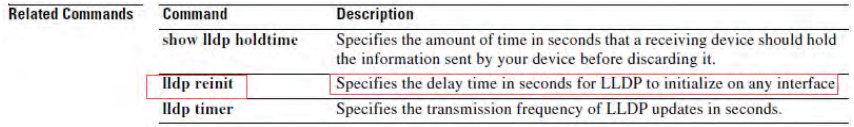
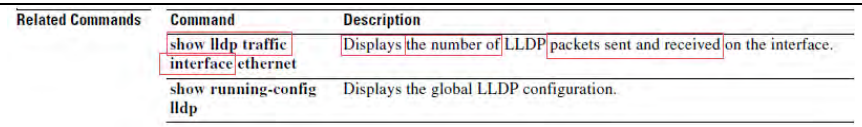
Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	Related Commands
	
	Command / **Description**
	ptp — Enables or disables PTP on an interface.
	ptp announce — Configures the interval between PTP announce messages on an interface or the number of PTP intervals before a timeout occurs on an interface.
	ptp delay-request minimum interval — Configures the minimum interval allowed between PTP delay-request messages when the port is in the master state.
	ptp sync interval — Configures the interval between PTP synchronization messages on an interface.
	
	Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 344.
		ptp announce interval
		
		The ptp announce interval command configures the interval between PTP announcement messages on or the number of PTP intervals before a timeout occurs. To disable this feature, use the no form of this command.
		
		Platform: Arad, FM6000
		Command Mode: Interface-Ethernet Configuration
		Interface-Port Channel Configuration
		
		Command Syntax
		`ptp announce interval log_interval`
		`no ptp announce interval`
		`default ptp announce interval`
		
		Parameters
		• *log_interval* The number of log seconds between PTP announcement message (base 2 log (seconds)). Value ranges from 0 to 4; default value is 1.
		
		Examples
		• This command shows how to configure the interval between PTP announce messages on an interface.
		`switch(config)# interface ethernet 5`
		`switch(config-if-Et5)# ptp announce interval 1`
		`switch(config-if-Et5)#`
		• This command removes the configured interval between PTP announce messages on interface Ethernet 5.
		`switch(config)# interface ethernet 5`
		`switch(config-if-Et5)# no ptp announce interval`
		`switch(config-if-Et5)#`
		
		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 315.
		
		See also Arista User Manual v. 4.12.3 (7/17/13), at 253; Arista User Manual, v. 4.11.1 (1/11/13), at 199.

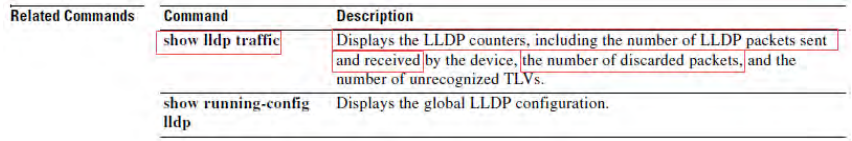
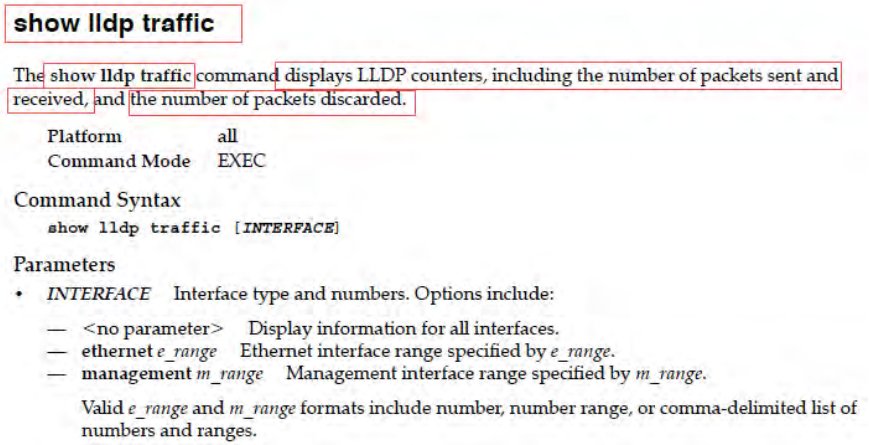
Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	**snmp-server user** To configure the Simple Network Management Protocol (SNMP) user information, use the **snmp-server user** command. To disable the configuration or to revert to factory defaults, use the **no** form of this command. **snmp-server user** *username* [*group-name*] [**auth** {**md5** | **sha**} *password* [**priv** [**aes-128**] *password*] [**localizedkey**] [**engineID** *id*] **no snmp-server user** *username* [*group-name*] [**auth** {**md5** | **sha**} *password* [**priv** [**aes-128**] *password*] [**localizedkey**] [**engineID** *id*] **Syntax Description** *username* — Name of the user. The name can be any case-sensitive, alphanumeric string up to 32 characters. *group-name* — (Optional) Name of the group. The name can be any case-sensitive, alphanumeric string up to 32 characters. **auth** — (Optional) Sets authentication parameters for the user. **md5** — Uses the MD5 algorithm for authentication. **sha** — Uses the SHA algorithm for authentication. *password* — User password. The password can be any case-sensitive, alphanumeric string up to 64 characters. If you configure the **localizedkey** keyword, the password can be any case-sensitive, alphanumeric string up to 130 characters **priv** — (Optional) Sets encryption parameters for the user. **aes-128** — (Optional) Sets the 128-byte AES algorithm for privacy. **localizedkey** — (Optional) Sets passwords in the localized key format. If you configure this keyword, the password can be any case-sensitive, alphanumeric string up to 130 characters. **engineID** *id* — (Optional) Configures the SNMP Engine ID for a notification target user. The engineID format is a 12-digit colon-separated decimal number. Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 394.	**snmp-server user** The **snmp-server user** command adds a user to a Simple Network Management Protocol (SNMP) group or modifies an existing user's parameters. To configure a remote user, specify the IP address or port number of the device where the user's remote SNMP agent resides. A remote agent's engine ID must be configured before remote users for that agent are configured. A user's authentication and privacy digests are derived from the engine ID and the user's password. The configuration command fails if the remote engine ID is not configured first. The **no snmp-server user** and **default snmp-server user** commands remove the user from an SNMP group by deleting the user command from *running-config*. Platform — all Command Mode — Global Configuration Command Syntax **snmp-server user** *user_name group_name* [*AGENT*] *VERSION* [*ENGINE*] [*SECURITY*] **no snmp-server user** *user_name group_name* [*AGENT*] *VERSION* **default snmp-server user** *user_name group_name* [*AGENT*] *VERSION* Parameters • *user_name* name of the user on the host that connects to the agent. • *group_name* name of the group to which the user is associated. • *AGENT* location of the host connecting to the SNMP agent. Configuration options include: — <no parameter> local SNMP agent. — **remote** *addr* [**udp-port** *p_num*] remote SNMP agent location (IP address, udp port). *addr* denotes the IP address; *p_num* denotes the udp port socket. (default port is 162). • *VERSION* SNMP version; options include: — **v1** SNMPv1. — v2c SNMPv2c. — **v3** SNMPv3; enables user-name match authentication. • *ENGINE* engine ID used to localize passwords. Available only if *VERSION* is v3. — <no parameter> Passwords localized by SNMP copy specified by *agent*. — **localized** *engineID* octet string of engineID. • *SECURITY* Specifies authentication and encryption levels. Available only if *VERSION* is v3. Encryption is available only when authentication is configured. — <no parameter> no authentication or encryption. — **auth** *a_meth a_pass* [**priv** *e_meth e_pass*] authentication and encryption parameters. *a-meth* authentication method: options are **md5** (HMAC-MD5-96) and **sha** (HMAC-SHA-96). *a-pass* authentication string for users receiving packets. *e-meth* encryption method: tions are **aes** (AES-128) and **des** (CBC-DES). *e-pass* encryption string for the users sending packets. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1999.

Copyright Registration Information	Cisco	Arista
		See also Arista User Manual v. 4.12.3 (7/17/13), at 1689; Arista User Manual, v. 4.11.1 (1/11/13), at 1374; Arista User Manual v. 4.10.3 (10/22/12), at 1141; Arista User Manual v. 4.9.3.2 (5/3/12), at 896; Arista User Manual v. 4.8.2 (11/18/11), at 703; Arista User Manual v. 4.7.3 (7/18/11), at 559.

Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	Examples
	This example shows how to display the EEE status on an interface:
	`switch# show interface ethernet2/6`
	`Ethernet2/6 is down (Link not connected)`
	`admin state is up, Dedicated Interface`
	`Hardware: 10000 Ethernet, address: 0022.5579.de41 (bia 001b.54c1.af5d)`
	`MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec`
	`reliability 255/255, txload 1/255, rxload 1/255`
	`Encapsulation ARPA, medium is broadcast`
	`auto-duplex, auto-speed, media type is 10G`
	`Beacon is turned off`
	`Auto-Negotiation is turned off`
	`Input flow-control is off, output flow-control is off`
	`Auto-mdix is turned off`
	`Rate mode is shared`
	`Switchport monitor is off`
	`EtherType is 0x8100`
	`EEE (efficient-ethernet) : n/a`
	`Last link flapped never`
	`Last clearing of "show interface" counters never`
	`0 interface resets`
	`30 seconds input rate 0 bits/sec, 0 packets/sec`
	`30 seconds output rate 0 bits/sec, 0 packets/sec`
	`Load-Interval #2: 5 minute (300 seconds)`
	
	Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 514.
		Example
		• This command assigns the MAC address of 001c.2804.17e1 to Ethernet interface 7, then displays interface parameters, including the assigned address.
		`switch(config)#interface ethernet 7`
		`switch(config-if-Et7)#mac-address 001c.2804.17e1`
		`switch(config-if-Et7)#show interface ethernet 7`
		`Ethernet3 is up, line protocol is up (connected)`
		`Hardware is Ethernet, address is 001c.2804.17e1 (bia 001c.7312.02e2)`
		`Description: b.e45`
		`MTU 9212 bytes, BW 10000000 Kbit`
		`Full-duplex, 10Gb/s, auto negotiation: off`
		`Last clearing of "show interface" counters never`
		`5 seconds input rate 7.84 kbps (0.0% with framing), 10 packets/sec`
		`5 seconds output rate 270 kbps (0.0% with framing), 24 packets/sec`
		`1363799 packets input, 222736140 bytes`
		`Received 0 broadcasts, 290904 multicast`
		`0 runts, 0 giants`
		`0 input errors, 0 CRC, 0 alignment, 0 symbol`
		`0 PAUSE input`
		`2264927 packets output, 2348747214 bytes`
		`Sent 0 broadcasts, 28573 multicast`
		`0 output errors, 0 collisions`
		`0 late collision, 0 deferred`
		`0 PAUSE output`
		`switch(config-if-Et7)#`
		
		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 437.
		
		See also Arista User Manual v. 4.12.3 (7/17/13), at 371; Arista User Manual, v. 4.11.1 (1/11/13), at 312; Arista User Manual v. 4.10.3 (10/22/12), at 270; Arista User Manual v. 4.9.3.2 (5/3/12), at 252.

Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 Related Commands / Command / Description show lldp tlv-select — Displays the LLDP TLV configuration. lldp tlv-select — Specifies the TLVs to send and receive in LLDP packets. Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 515.	**lldp tlv-select** The lldp tlv-select command allows the user to specify the TLVs to send and receive in LLDP packets. The available TLVs are management-address, port-description, port-vlan, system-capabilities, system-description, and system-name. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 592. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 465; Arista User Manual, v. 4.11.1 (1/11/13), at 383.
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 Related Commands / Command / Description show lldp traffic interface ethernet — Displays the number of LLDP packets sent and received on the interface. show running-config lldp — Displays the global LLDP configuration. lldp transmit — Enables the transmission of LLDP packets on an interface. lldp receive — Enables the reception of LLDP packets on an interface. Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 522.	**lldp transmit** The lldp transmit command enables the transmission of LLDP packets on an interface. After you globally enable LLDP, it is enabled on all supported interfaces by default. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 593. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 466; Arista User Manual, v. 4.11.1 (1/11/13), at 384.
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 Related Commands / Command / Description show lldp holdtime — Specifies the amount of time in seconds that a receiving device should hold the information sent by your device before discarding it. lldp reinit — Specifies the delay time in seconds for LLDP to initialize on any interface. lldp timer — Specifies the transmission frequency of LLDP updates in seconds. Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 522.	12.3.3.2 Setting the LLDP Hold Time The lldp holdtime command specifies the amount of time in seconds that a receiving device should hold the information sent by the device before discarding it. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 578. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 450; Arista User Manual, v. 4.11.1 (1/11/13), at 368

Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 Related Commands Command — Description show lldp holdtime — Specifies the amount of time in seconds that a receiving device should hold the information sent by your device before discarding it. lldp reinit — Specifies the delay time in seconds for LLDP to initialize on any interface lldp timer — Specifies the transmission frequency of LLDP updates in seconds. Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 522.	**lldp reinit** The lldp reinit command specifies the delay time in seconds for LLDP to initialize on any interface. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 589. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 462; Arista User Manual, v. 4.11.1 (1/11/13), at 380.
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 Related Commands Command — Description show lldp traffic interface ethernet — Displays the number of LLDP packets sent and received on the interface. show running-config lldp — Displays the global LLDP configuration. Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 527.	**show lldp traffic** The show lldp traffic command displays LLDP counters, including the number of packets sent and received, and the number of packets discarded. Platform all Command Mode EXEC Command Syntax `show lldp traffic [INTERFACE]` Parameters • *INTERFACE* Interface type and numbers. Options include: — <no parameter> Display information for all interfaces. — ethernet *e_range* Ethernet interface range specified by *e_range*. — management *m_range* Management interface range specified by *m_range*. Valid *e_range* and *m_range* formats include number, number range, or comma-delimited list of numbers and ranges. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 599. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 472; Arista User Manual, v. 4.11.1 (1/11/13), at 390.

Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 Related Commands Command: show lldp traffic — Description: Displays the LLDP counters, including the number of LLDP packets sent and received by the device, the number of discarded packets, and the number of unrecognized TLVs. Command: show running-config lldp — Description: Displays the global LLDP configuration. Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 529.	 **show lldp traffic** The show lldp traffic command displays LLDP counters, including the number of packets sent and received, and the number of packets discarded. Platform all Command Mode EXEC Command Syntax `show lldp traffic [INTERFACE]` Parameters • *INTERFACE* Interface type and numbers. Options include: — <no parameter> Display information for all interfaces. — ethernet *e_range* Ethernet interface range specified by *e_range*. — management *m_range* Management interface range specified by *m_range*. Valid *e_range* and *m_range* formats include number, number range, or comma-delimited list of numbers and ranges. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 599. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 472; Arista User Manual, v. 4.11.1 (1/11/13), at 390.

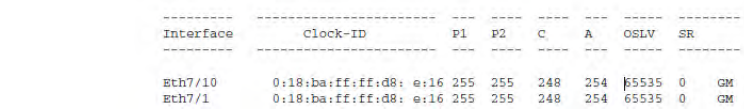
Copyright Registration Information	Cisco	Arista

Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	show ptp clock
	
	To display the Precision Time Protocol (PTP) clock information, use the **show ptp clock** command.
	
	show ptp clock
	
	Syntax Description This command has no arguments or keywords.
	
	Defaults None
	
	Command Modes Any command mode
	
	SupportedUserRoles network-admin
	network-operator
	vdc-admin
	vdc-operator
	
	Command History
	Release 5.2(1) — **Modification** This command was introduced.
	
	Usage Guidelines This command does not require a license.
	
	Examples This example shows how to display the PTP clock information:
	`switch# show ptp clock`
	`PTP Device Type: Boundary clock`
	`Clock Identity : 0:18:ba:ff:ff:d8: e:17`
	`Clock Domain: 0`
	`Number of PTP ports: 2`
	`Priority1 : 255`
	`Priority2 : 255`
	`Clock Quality:`
	`Class : 248`
	`Accuracy : 254`
	`Offset (log variance) : 65535`
	`Offset From Master : 0`
	`Mean Path Delay : 0`
	`Steps removed : 1`
	`Local clock time:Sun Jan 15 20:57:29 2011`
	
	Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 601.
		Show PTP Clock and Offset
		
		To display the Precision Time Protocol (PTP) local clock and offset, use the show ptp clock command.
		
		• The show ptp clock command displays the Precision Time Protocol (PTP) local clock and offset.
		`switch#show ptp clock`
		`PTP Mode: Boundary Clock`
		`Clock Identity: 0x00:1c:73:ff:ff:1e:83:24`
		`Clock Domain: 1`
		`Number of PTP ports: 24`
		`Priority1: 128`
		`Priority2: 128`
		`Clock Quality:`
		`Class: 248`
		`Accuracy: 0x30`
		`OffsetScaledLogVariance: 0xffff`
		`Offset From Master: 0`
		`Mean Path Delay: 0`
		`Steps Removed: 0`
		`switch#`
		
		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 275.
		
		See also Arista User Manual v. 4.12.3 (7/17/13), at 217.

Copyright Registration Information	Cisco	Arista

Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	show ptp clock foreign-masters-record
	
	To display information about the state of foreign masters known to the Precision Time Protocol (PTP) process, use the **show ptp clocks foreign-masters-record** command.
	
	show ptp clock foreign-masters-record {interface [ethernet]}
	
	Syntax DescriptionT
	interface — Specifies an interface.
	ethernet — (Optional) Specifies an Ethernet interface.
	
	Defaults
	None
	
	Command Modes
	Any command mode
	
	SupportedUserRoles
	network-admin
	network-operator
	vdc-admin
	vdc-operator
	
	Command History
	Release — **Modification**
	5.2(1) — This command was introduced.
	
	Usage Guidelines
	This command does not require a license.
	
	Examples
	This example shows how to display information about the state of foreign masters known to the PTP process:
	`switch# show ptp clock foreign-masters-record interface ethernet 7/1`
	`RP/0/0/CPU0:demo#show ptp clocks foreign-masters`
	`P1=Priority1, P2=Priority2, C=Class, A=Accuracy,`
	`OSLV=Offset-Scaled-Log-Variance, SR=Steps-Removed`
	`GM=Is grandmaster`
	
	`Interface Clock-ID P1 P2 C A OSLV SR`
	`Eth7/10 0:18:ba:ff:ff:d8: e:16 255 255 248 254 65535 0 GM`
	`Eth7/1 0:18:ba:ff:ff:d8: e:16 255 255 248 254 65535 0 GM`
	
	Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 603.
		Show PTP Foreign Master
		
		To display information about the state of foreign masters known to the Precision Time Protocol (PTP) process, use the show ptp foreign-master-record command.
		
		• The show ptp foreign-master-records command displays information about the state of foreign masters known to the PTP process.
		`switch# show ptp clocks foreign-masters-record`
		`No Foreign Master Records`
		`switch#`
		
		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 277.
		
		See also Arista User Manual v. 4.12.3 (7/17/13), at 219-220.

Copyright Registration Information	Cisco	Arista

Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	Examples
	This example shows how to display information about the state of foreign masters known to the PTP process:
	`switch# show ptp clock foreign-masters-record interface ethernet 7/1`
	`RP/0/0/CPU0:demo#show ptp clocks foreign-masters`
	`P1=Priority1, P2=Priority2, C=Class, A=Accuracy,`
	`OSLV=Offset-Scaled-Log-Variance, SR=Steps-Removed`
	`GM=Is grandmaster`
	 
	`Interface Clock-ID P1 P2 C A OSLV SR`
	`Eth7/10 0:18:ba:ff:ff:d8: e:16 255 255 248 254 65535 0 GM`
	`Eth7/1 0:18:ba:ff:ff:d8: e:16 255 255 248 254 65535 0 GM`
	
	Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 603.
		Examples
		• This command shows how to display information about the state of foreign masters known to the PTP process.
		`switch# show ptp clocks foreign-masters-record`
		`No Foreign Master Records`
		`switch#`
		
		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 349.
		
		See also Arista User Manual v. 4.12.3 (7/17/13), at 282; Arista User Manual, v. 4.11.1 (1/11/13), at 228.

Copyright Registration Information	Cisco	Arista

Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	show ptp parent
	
	To display information about the parent and grand master of the Precision Time Protocol (PTP) clock, use the **show ptp parent** command.
	
	show ptp parent
	
	Syntax Description This command has no arguments or keywords.
	
	Defaults None
	
	Command Modes Any command mode
	
	SupportedUserRoles network-admin
	network-operator
	vdc-admin
	vdc-operator
	
	Command History
	Release 5.2(1) — **Modification** This command was introduced.
	
	Usage Guidelines This command does not require a license.
	
	Examples This example shows how to display information about the parent and grand master of the PTP clock:
	`switch# show ptp parent`
	`Parent Clock:`
	`Parent Clock Identity: 0:18:ba:ff:ff:d8: e:16`
	`Parent Port Number: 1546`
	`Observed Parent Offset (log variance): N/A`
	`Observed Parent Clock Phase Change Rate: N/A`
	
	`Grandmaster Clock:`
	`Grandmaster Clock Identity: 0:18:ba:ff:ff:d8: e:16`
	`Grandmaster Clock Quality:`
	`Class: 248`
	`Accuracy: 254`
	`Offset(log variance): 65535`
	`Priority1: 255`
	`Priority2: 255`
	
	Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 607.
		Show PTP Parent Information
		
		To display information about the parent and grand master of the Precision Time Protocol (PTP) clock, use the show ptp parent command.
		
		• The show ptp parent command displays information about the parent and grand master of the Precision Time Protocol (PTP) clock.
		`switch# show ptp parent`
		`Parent Clock:`
		`Parent Clock Identity: 0x00:1c:73:ff:ff:00:72:40`
		`Parent Port Number: 0`
		`Parent IP Address: N/A`
		`Observed Parent Offset (log variance): N/A`
		`Observed Parent Clock Phase Change Rate: N/A`
		
		`Grandmaster Clock:`
		`Grandmaster Clock Identity: 0x00:1c:73:ff:ff:00:72:40`
		`Grandmaster Clock Quality:`
		`Class: 248`
		`Accuracy: 0x30`
		`OffsetScaledLogVariance: 0xffff`
		`Priority1 128`
		`Priority2 128`
		`switch#`
		
		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 275.
		
		See also Arista User Manual v. 4.12.3 (7/17/13), at 217.

Copyright Registration Information	Cisco	Arista

Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	show ptp parent
	
	To display information about the parent and grand master of the Precision Time Protocol (PTP) clock, use the **show ptp parent** command.
	
	show ptp parent
	
	Syntax Description This command has no arguments or keywords.
	
	Defaults None
	
	Command Modes Any command mode
	
	SupportedUserRoles network-admin
	network-operator
	vdc-admin
	vdc-operator
	
	Command History
	Release: 5.2(1) — Modification: This command was introduced.
	
	Usage Guidelines This command does not require a license.
	
	Examples This example shows how to display information about the parent and grand master of the PTP clock:
	`switch# show ptp parent`
	`Parent Clock:`
	`Parent Clock Identity: 0:18:ba:ff:ff:d8: e:16`
	`Parent Port Number: 1546`
	`Observed Parent Offset (log variance): N/A`
	`Observed Parent Clock Phase Change Rate: N/A`
	
	`Grandmaster Clock:`
	`Grandmaster Clock Identity: 0:18:ba:ff:ff:d8: e:16`
	`Grandmaster Clock Quality:`
	`Class: 248`
	`Accuracy: 254`
	`Offset (log variance): 65535`
	`Priority1: 255`
	`Priority2: 255`
	
	Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 607.
		show ptp parent
		
		The show ptp parent command displays information about the parent and grand master of the Precision Time Protocol (PTP) clock.
		
		Platform Arad, FM6000
		Command Mode Privileged EXEC
		
		Command Syntax
		`show ptp parent`
		
		Examples
		• This command shows how to display information about the parent and master of the PTP clock.
		`switch# show ptp parent`
		`Parent Clock:`
		`Parent Clock Identity: 0x00:1c:73:ff:ff:00:72:40`
		`Parent Port Number: 0`
		`Parent IP Address: N/A`
		`Observed Parent Offset (log variance): N/A`
		`Observed Parent Clock Phase Change Rate: N/A`
		
		`Grandmaster Clock:`
		`Grandmaster Clock Identity: 0x00:1c:73:ff:ff:00:72:40`
		`Grandmaster Clock Quality:`
		`Class: 248`
		`Accuracy: 0x30`
		`OffsetScaledLogVariance: 0xffff`
		`Priority1: 128`
		`Priority2: 128`
		`switch#`
		
		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 352.
		
		See also Arista User Manual v. 4.12.3 (7/17/13), at 285; Arista User Manual, v. 4.11.1 (1/11/13), at 231.

Copyright Registration Information	Cisco	Arista

Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	show ptp time-property
	
	To display the Precision Time Protocol (PTP) clock properties, use the **show ptp time-property** command.
	
	show ptp time-property
	
	Syntax Description This command has no arguments or keywords.
	
	Defaults None
	
	Command Modes Any command mode
	
	SupportedUserRoles network-admin
	network-operator
	vdc-admin
	vdc-operator
	
	Command History
	Release 5.2(1) — **Modification** This command was introduced.
	
	Usage Guidelines This command does not require a license.
	
	Examples This example shows how to display the PTP clock properties:
	`switch# show ptp time-property`
	`PTP CLOCK TIME PROPERTY:`
	`Current UTC offset valid: 0`
	`Current UTC offset: 33`
	`Leap59: 0`
	`Leap61: 0`
	`Time Traceable: 0`
	`Frequency Traceable: 0`
	`PTP Timescale: 0`
	`Time Source: 0xA0(internal Osccilator)`
	
	Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 611.
		Show PTP Clock Properties
		
		To display the Precision Time Protocol (PTP) clock properties, use the show ptp time-property command.
		
		• The show ptp time-property command displays the Precision Time Protocol (PTP) clock properties.
		`switch# show ptp time-property`
		`Current UTC offset valid: False`
		`Current UTC offset: 0`
		`Leap 59: False`
		`Leap 61: False`
		`Time Traceable: False`
		`Frequency Traceable: False`
		`PTP Timescale: False`
		`Time Source: 0x0`
		`switch#`
		
		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 275-76.
		
		See also Arista User Manual v. 4.12.3 (7/17/13), at 218.

Copyright Registration Information	Cisco	Arista

Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	show ptp time-property
	
	To display the Precision Time Protocol (PTP) clock properties, use the **show ptp time-property** command.
	
	show ptp time-property
	
	Syntax Description This command has no arguments or keywords.
	
	Defaults None
	
	Command Modes Any command mode
	
	SupportedUserRoles network-admin
	network-operator
	vdc-admin
	vdc-operator
	
	Command History
	Release: 5.2(1)
	Modification: This command was introduced.
	
	Usage Guidelines This command does not require a license.
	
	Examples This example shows how to display the PTP clock properties:
	`switch# show ptp time-property`
	`PTP CLOCK TIME PROPERTY:`
	`Current UTC offset valid: 0`
	`Current UTC offset: 33`
	`Leap59: 0`
	`Leap61: 0`
	`Time Traceable: 0`
	`Frequency Traceable: 0`
	`PTP Timescale: 0`
	`Time Source: 0xA0(internal Osccilator)`
	
	Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 611.
		show ptp time-property
		
		The show ptp time-property command displays the Precision Time Protocol (PTP) clock properties.
		
		Platform: Arad, FM6000
		Command Mode: Privileged EXEC
		
		Command Syntax
		`show ptp time-property`
		
		Examples
		• This command shows the PTP clock properties.
		`switch# show ptp time-property`
		`Current UTC offset valid: False`
		`Current UTC offset: 0`
		`Leap 59: False`
		`Leap 61: False`
		`Time Traceable: False`
		`Frequency Traceable: False`
		`PTP Timescale: False`
		`Time Source: 0x0`
		`switch#`
		
		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 354.
		
		See also Arista User Manual v. 4.12.3 (7/17/13), at 287; Arista User Manual, v. 4.11.1 (1/11/13), at 233.

Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	Examples
	This example shows how to display the SNMP information:
	`switch(config)# show snmp`
	`sys contact:`
	`sys location: anyplace, Anywhere`
	
	`0 SNMP packets input`
	`0 Bad SNMP versions`
	`0 Unknown community name`
	`0 Illegal operation for community name supplied`
	`0 Encoding errors`
	`0 Number of requested variables`
	`0 Number of altered variables`
	`0 Get-request PDUs`
	`0 Get-next PDUs`
	`0 Set-request PDUs`
	`0 SNMP packets output`
	`0 Too big errors`
	`0 No such name errors`
	`0 Bad values errors`
	`0 General errors`
	
	Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 634.
		Example
		• This command configures *xyz-1234* as the chassis-ID string, then displays the result.
		`switch(config)#snmp-server chassis-id xyz-1234`
		`switch(config)#show snmp`
		`Chassis: xyz-1234` *<---chassis ID*
		
		`8 SNMP packets input`
		`0 Bad SNMP version errors`
		`0 Unknown community name`
		`0 Illegal operation for community name supplied`
		`0 Encoding errors`
		`8 Number of requested variables`
		`0 Number of altered variables`
		`4 Get-request PDUs`
		`4 Get-next PDUs`
		`0 Set-request PDUs`
		`21 SNMP packets output`
		`0 Too big errors`
		`0 No such name errors`
		`0 Bad value errors`
		`0 General errors`
		`8 Response PDUs`
		`0 Trap PDUs`
		`SNMP logging: enabled`
		`Logging to taccon.162`
		`SNMP agent enabled`
		`switch(config)#`
		
		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 354.
		
		See also Arista User Manual v. 4.12.3 (7/17/13), at 1657-58; Arista User Manual, v. 4.11.1 (1/11/13), at 1344-45; Arista User Manual v. 4.10.3 (10/22/12), at 1111; Arista User Manual v. 4.9.3.2 (5/3/12), at 867; Arista User Manual v. 4.8.2 (11/18/11), at 678; Arista User Manual v. 4.7.3 (7/18/11), at 549.

Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	show snmp engineID
	
	To display the Simple Network Management Protocol (SNMP) engine ID, use the **show snmp engineID** command.
	
	show snmp engineID
	
	Syntax Description This command has no arguments or keywords.
	
	Defaults None
	
	Command Modes Any command mode
	
	SupportedUserRoles network-admin
	network-operator
	vdc-admin
	vdc-operator
	
	Command History
	Release — **Modification**
	4.0(1) — This command was introduced.
	
	Usage Guidelines This command does not require a license.
	
	Examples This example shows how to display the SNMP engine ID:
	`switch(config)# show snmp engineID`
	`Local SNMP engineID: [Hex] 8000009030005300A0B0C`
	`[Dec] 128:000:000:009:003:000:005:048:010:011:012`
	
	Related Commands
	Command — **Description**
	snmp-server user — Configures SNMP target notification users.
	
	Cisco Nexus 7000 Series NX-OS System Management Command Reference (2013), at 639.
		show snmp engineID
		
		The show snmp engineID command displays the identification of the local Simple Network Management Protocol (SNMP) engine and of all remote engines that are configured on the switch.
		
		Platform all
		Command Mode EXEC
		
		Command Syntax
		`show snmp engineID`
		
		Example
		• This command displays the ID of the local SNMP engine.
		`switch>show snmp engineid`
		`Local SNMP EngineID: f5717f001c730436d700`
		`switch>`
		
		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1978.
		
		See also Arista User Manual v. 4.12.3 (7/17/13), at 1668; Arista User Manual, v. 4.11.1 (1/11/13), at 1355; Arista User Manual v. 4.10.3 (10/22/12), at 1122; Arista User Manual v. 4.9.3.2 (5/3/12), at 878; Arista User Manual v. 4.8.2 (11/18/11), at 686; Arista User Manual v. 4.7.3 (7/18/11), at 542.

Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	**Precision Time Protocol** The Precision Time Protocol (PTP) is a time synchronization protocol for nodes distributed across a network. Its hardware timestamp feature provides greater accuracy than other time synchronization protocols such as Network Time Protocol (NTP). For more information about PTP, see Chapter 4, "Configuring PTP." Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 1-3.	5.3.2 Precision Time Protocol (PTP) The Precision Time Protocol (PTP) can substantially enhance the accuracy of real-time clocks in networked devices by providing sub-microsecond clock synchronization. Inbound clock signals are organized into a master-slave hierarchy. PTP identifies the switch port that is connected to the device with the most precise clock. This clock is referred to as the master clock. All the other devices on the network synchronize their clocks with the master and are referred to as slaves. The master clock sends out a sync message every second. The slave clock sends a delay request message to the master clock noting the time it was sent in order to measure and eliminate packet delays. The master clock then replies with the time stamp the delay message was received. The slave clock then computes the master clock time compensated for delays and finalizes synchronization. Constantly exchanged timing messages ensure continued synchronization. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 270. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 213; Arista User Manual, v. 4.11.1 (1/11/13), at 163.
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	**SNMP** The Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network. For more information, see Chapter 11, "Configuring SNMP." Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 1-5.	**37.2 SNMP Conceptual Overview** Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a standardized framework and a common language to monitor and manage network devices. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1961. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1651; Arista User Manual, v. 4.11.1 (1/11/13), at 1338; Arista User Manual v. 4.10.3 (10/22/12), at 1105; Arista User Manual v. 4.9.3.2 (5/3/12), at 861; Arista User Manual v. 4.8.2 (11/18/11), at 673; Arista User Manual v. 4.7.3 (7/18/11), at 529.
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	**SNMP** The Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network. For more information, see Chapter 11, "Configuring SNMP." Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 1-5.	Chapter 37 SNMP SNMP is an application-layer protocol that provides a standardized framework and a common language to monitor and manage network devices. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 43. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 37; Arista User Manual, v. 4.11.1 (1/11/13), at 31Arista User Manual v. 4.10.3 (10/22/12), at 28; Arista User Manual v. 4.9.3.2 (5/3/12), at 24; Arista User Manual v. 4.8.2 (11/18/11), at 20; Arista User Manual v. 4.7.3 (7/18/11), at 18.

<table>
<tr>
<td>Cisco NX-OS 6.2

Effective date of registration: 11/13/2014</td>
<td>

Configuring the NTP Source IP Address

NTP sets the source IP address for all NTP packets based on the address of the interface through which the NTP packets are sent. You can configure NTP to use a specific source IP address.

To configure the NTP source IP address, use the following command in global configuration mode:

Command	Purpose
[no] ntp source *ip-address* **Example:** switch(config)# ntp source 192.0.2.1	Configures the source IP address for all NTP packets. The *ip-address* can be in IPv4 or IPv6 format.

Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 3-16.

</td>
<td>

Configure the Source IP

To configure the source IP address for all PTP packets, use the ptp source ip command.

- The ptp source ip command configures the source IP address of 10.0.2.1 for all PTP packets.

```
switch(config)# ptp source ip 10.0.2.1
switch(config)#
```

Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 272.

See also Arista User Manual v. 4.12.3 (7/17/13), at 215.

</td>
</tr>
<tr>
<td>Cisco NX-OS 6.2

Effective date of registration: 11/13/2014</td>
<td>

Configuration Examples for NTP

This example shows how to configure an NTP server and peer, enable NTP authentication, enable NTP logging, and then save the configuration in startup so that it is saved across reboots and restarts:

```
switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp server 192.0.2.105 key 42
switch(config)# ntp peer 2001:0db8::4101
switch(config)# show ntp peers
-------------------------------------------------------
  Peer IP Address                Serv/Peer
-------------------------------------------------------
  2001:db8::4101                 Peer (configured)
  192.0.2.105                    Server (configured)
switch(config)# ntp authentication-key 42 md5 aNiceKey
switch(config)# show ntp authentication-keys
-----------------------------
 Auth key         MD5 String
-----------------------------
  42                    aNicekey
switch(config)# ntp trusted-key 42
switch(config)# show ntp trusted-keys
Trusted Keys:
42
switch(config)# ntp authenticate
switch(config)# show ntp authentication-status
Authentication enabled.
switch(config)# ntp logging
switch(config)# show ntp logging
NTP logging enabled.
switch(config)# copy running-config startup-config
[########################################] 100%
switch(config)#
```

Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 3-25.

</td>
<td>

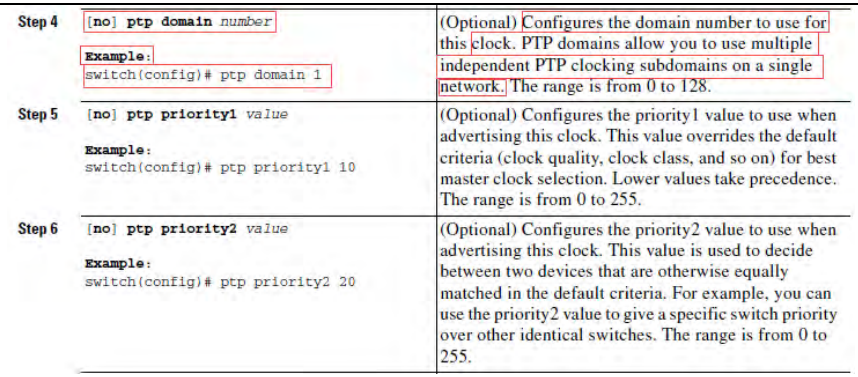
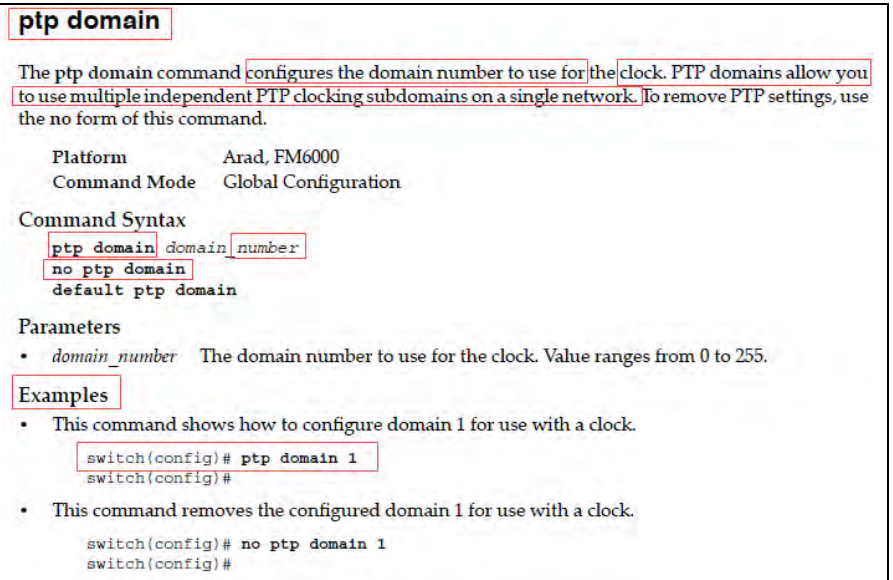
Example

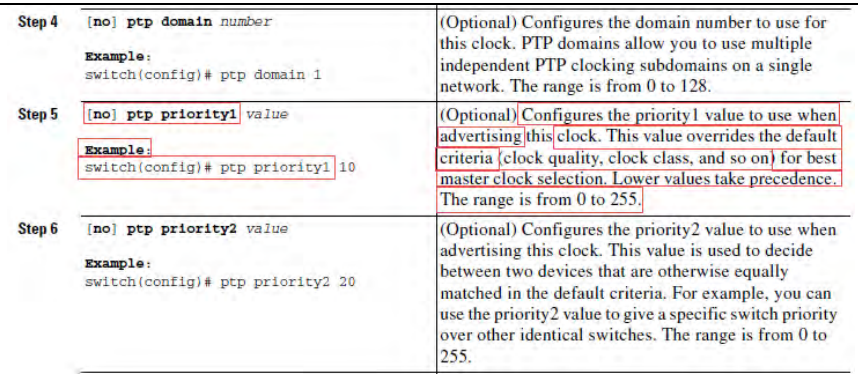
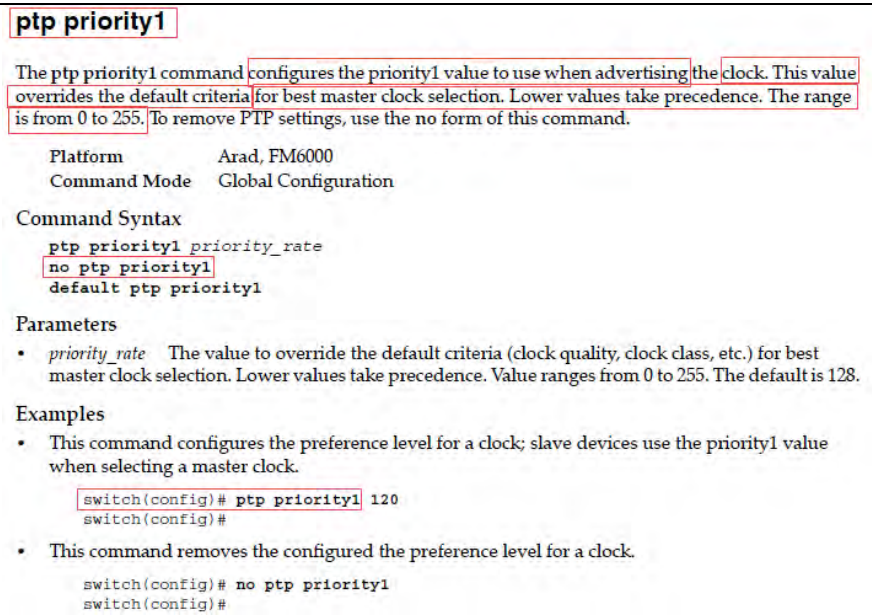
- These commands configure the switch to authenticate NTP packets using key 328 with the plaintext password "timeSync."

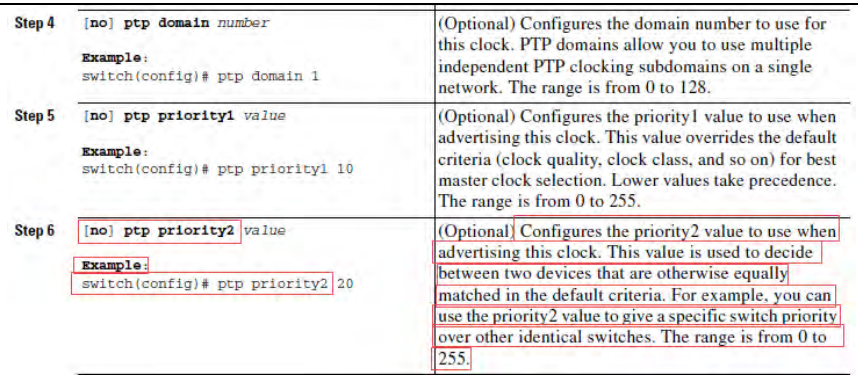
```
switch(config)# ntp authentication-key 328 md5 timeSync
switch(config)# ntp trusted key 328
switch(config)# ntp authenticate
switch(config)#
```

Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 270.

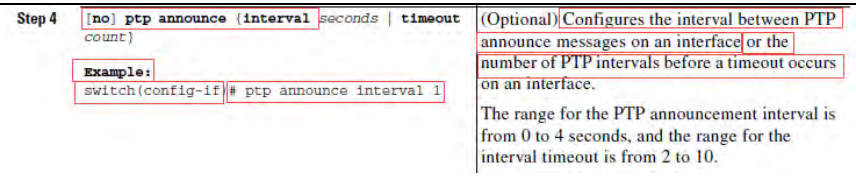
</td>
</tr>
</table>

Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 4-6.	 Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 319. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 257; Arista User Manual, v. 4.11.1 (1/11/13), at 204.

Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	 Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 4-6.	 Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 326. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 318; Arista User Manual v. 4.12.3 (7/17/13), at 262; Arista User Manual, v. 4.11.1 (1/11/13), at 208.

Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	
	Step 4 `[no] ptp domain number` — Example: `switch(config)# ptp domain 1` — (Optional) Configures the domain number to use for this clock. PTP domains allow you to use multiple independent PTP clocking subdomains on a single network. The range is from 0 to 128.
	Step 5 `[no] ptp priority1 value` — Example: `switch(config)# ptp priority1 10` — (Optional) Configures the priority1 value to use when advertising this clock. This value overrides the default criteria (clock quality, clock class, and so on) for best master clock selection. Lower values take precedence. The range is from 0 to 255.
	Step 6 `[no] ptp priority2 value` — Example: `switch(config)# ptp priority2 20` — (Optional) Configures the priority2 value to use when advertising this clock. This value is used to decide between two devices that are otherwise equally matched in the default criteria. For example, you can use the priority2 value to give a specific switch priority over other identical switches. The range is from 0 to 255.
	
	Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 4-6.
		ptp priority2
		
		The ptp priority2 command configures the priority2 value to use when advertising this clock. This value is used to decide between two devices that are otherwise equally matched in the default criteria. For example, you can use the priority2 value to give a specific switch priority over other identical switches. The range is from 0 to 255. To remove PTP settings, use the no form of this command.
		
		Platform Arad, FM6000
		Command Mode Global Configuration
		
		Command Syntax
		`ptp priority2 priority_rate`
		`no ptp priority2`
		`default ptp priority2`
		
		Parameters
		• *priority_rate* Sets a secondary preference level for a clock; slave devices use the priority2 value when selecting a master clock. Value ranges from 0 to 255.
		
		Examples
		• This command sets a secondary preference level for a clock to 128.
		`switch(config)# ptp priority2 128`
		`switch(config)#`
		• This command removes the secondary preference level for a clock.
		`switch(config)# no ptp priority2`
		`switch(config)#`
		
		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 327.
		
		See also Arista User Manual v. 4.13.6F (4/14/2014), at 319; Arista User Manual v. 4.12.3 (7/17/13), at 263; Arista User Manual, v. 4.11.1 (1/11/13), at 209.

Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	**BEFORE YOU BEGIN** Make sure that you are in the correct VDC. To change the VDC, use the **switchto vdc** command. Make sure that you have globally enabled PTP on the device and configured the source IP address for PTP communication. Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 4-7.	**ptp delay-req interval** The ptp delay-req interval command specifies the time recommended to the slave devices to send delay request messages. You must enable PTP on the switch first and configure the source IP address for PTP communication. To remove the minimum interval configuration for PTP delay-request messages, use the no form of this command. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 318. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 256; Arista User Manual, v. 4.11.1 (1/11/13), at 202.

Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	
	Step 4 `[no] ptp announce {interval` *seconds* `| timeout` *count*`}`
	(Optional) Configures the interval between PTP announce messages on an interface or the number of PTP intervals before a timeout occurs on an interface.
	The range for the PTP announcement interval is from 0 to 4 seconds, and the range for the interval timeout is from 2 to 10.
	Example:
	`switch(config-if)# ptp announce interval 1`
	
	Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 4-8.
		ptp announce interval
		The **ptp announce interval** command configures the interval between PTP announcement messages on or the number of PTP intervals before a timeout occurs. To disable this feature, use the no form of this command.
		Platform Arad, FM6000
		Command Mode Interface-Ethernet Configuration
		Interface-Port Channel Configuration
		Command Syntax
		`ptp announce interval log_interval`
		`no ptp announce interval`
		`default ptp announce interval`
		Parameters
		• *log_interval* The number of log seconds between PTP announcement message (base 2 log (seconds)). Value ranges from 0 to 4; default value is 1.
		Examples
		• This command shows how to configure the interval between PTP announce messages on an interface.
		`switch(config)# interface ethernet 5`
		`switch(config-if-Et5)# ptp announce interval 1`
		`switch(config-if-Et5)#`
		• This command removes the configured interval between PTP announce messages on interface Ethernet 5.
		`switch(config)# interface ethernet 5`
		`switch(config-if-Et5)# no ptp announce interval`
		`switch(config-if-Et5)#`
		
		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 315.
		
		See also Arista User Manual v. 4.12.3 (7/17/13), at 252; Arista User Manual, v. 4.11.1 (1/11/13), at 199.

Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	Step 5	[no] ptp delay-request minimum interval *seconds* **Example:** switch(config-if)# ptp delay-request minimum interval 3
		(Optional) Configures the minimum interval allowed between PTP delay-request messages when the port is in the master state. The range is from –1 to 6 seconds.
	Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 4-8.	
	ptp delay-req interval The **ptp delay-req interval** command specifies the time recommended to the slave devices to send delay request messages. You must enable PTP on the switch first and configure the source IP address for PTP communication. To remove the minimum interval configuration for PTP delay-request messages, use the no form of this command. **Platform** Arad, FM6000 **Command Mode** Interface-Ethernet Configuration Interface-Port Channel Configuration Command Syntax **ptp delay-req interval** *log_interval* **no ptp delay-req interval** **default ptp delay-req interval** Parameters • *log_interval* The range is -1 second to 8 seconds. The default is 5 log(seconds). Examples • This command shows how to configure the minimum interval allowed between PTP delay-request messages. switch(config)# **interface ethernet 5** switch(config-if-Et5)# **ptp delay-request interval 3** switch(config-if-Et5)# • This command removes the configured minimum interval allowed between PTP delay-request messages. switch(config)# **interface ethernet 5** switch(config-if-Et5)# **no ptp delay-request interval** switch(config-if-Et5)#	
	Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 318. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 256; Arista User Manual, v. 4.11.1 (1/11/13), at 202.	

<table>
<tr>
<td>Cisco NX-OS 6.2

Effective date of registration: 11/13/2014</td>
<td>
Verifying the PTP Configuration
To display the PTP configuration, perform one of the following tasks:
<table>
<tr><th>Command</th><th>Purpose</th></tr>
<tr><td>show ptp brief</td><td>Displays the PTP status.</td></tr>
<tr><td>show ptp clock</td><td>Displays the properties of the local clock.</td></tr>
<tr><td>show ptp clock foreign-masters record [interface interface slot/port]</td><td>Displays the state of foreign masters known to the PTP process. For each foreign master, the output displays the clock identity, basic clock properties, and whether the clock is being used as a grandmaster.</td></tr>
<tr><td>show ptp corrections</td><td>Displays the last few PTP corrections.</td></tr>
<tr><td>show ptp parent</td><td>Displays the properties of the PTP parent.</td></tr>
<tr><td>show ptp port interface interface slot/port</td><td>Displays the status of the PTP port.</td></tr>
<tr><td>show ptp time-property</td><td>Displays the properties of the PTP clock.</td></tr>
</table>

Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 4-9.
</td>
<td>
show ptp foreign-master-record

The show ptp foreign-master-record command displays information about the state of foreign masters known to the Precision Time Protocol (PTP) process.

Platform Arad, FM6000
Command Mode EXEC

Command Syntax
show ptp foreign-master-record

Examples
• This command shows how to display information about the state of foreign masters known to the PTP process.

switch# show ptp clocks foreign-masters-record
No Foreign Master Records
switch#

Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 349.

See also Arista User Manual v. 4.12.3 (7/17/13), at 282; Arista User Manual, v. 4.11.1 (1/11/13), at 228.
</td>
</tr>
</table>

Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	**SNMP Functional Overview** The SNMP framework consists of three parts: • An SNMP manager—The system used to control and monitor the activities of network devices using SNMP. • An SNMP agent—The software component within the managed device that maintains the data for the device and reports these data, as needed, to managing systems. Cisco NX-OS supports the agent and MIB. To enable the SNMP agent, you must define the relationship between the manager and the agent. • A managed information base (MIB)—The collection of managed objects on the SNMP agent. SNMP is defined in RFCs 3411 to 3418. Cisco NX-OS supports SNMPv1, SNMPv2c, and SNMPv3. Both SNMPv1 and SNMPv2c use a community-based form of security. Cisco NX-OS supports SNMP over IPv6. Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 11-2.	37.2.3 SNMP Versions Arista switches support the following SNMP versions: • **SNMPv1**: The Simple Network Management Protocol, defined in RFC 1157. Security is based on community strings. • **SNMPv2c**: Community-string based Administrative Framework for SNMPv2, defined in RFC 1901 RFC 1905, and RFC 1906. SNMPv2c uses the community-based security model of SNMPv1. • **SNMPv3**: Version 3 is an interoperable standards-based protocol defined in RFCs 2273 to 2275. SNMPv3 provides secure access to devices by authenticating and encrypting packets. The security features provided in SNMPv3 are as follows: — *Message integrity*: Ensures packets are not tampered with in transit. — *Authentication*: Determines the message is received from a valid source. — *Encryption*: Scrambling packet contents to prevent an unauthorized source from learning it. Both SNMPv1 and SNMPv2c use a community-based form of security. The community of managers able to access the agent MIB is controlled by a password. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 349. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1891;Arista User Manual v. 4.12.3 (7/17/13), at 1654; Arista User Manual, v. 4.11.1 (1/11/13), at 1341; Arista User Manual v. 4.10.3 (10/22/12), at 1107; Arista User Manual v. 4.9.3.2 (5/3/12), at 863; Arista User Manual v. 4.8.2 (11/18/11), at 675; Arista User Manual v. 4.7.3 (7/18/11), at 531.

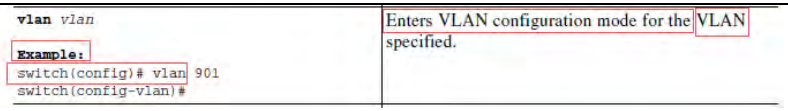
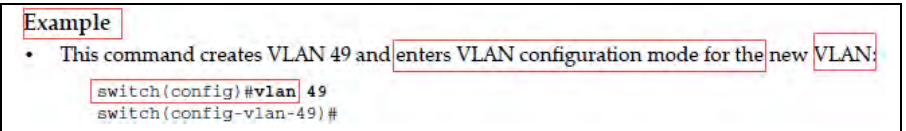
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	**SNMP Functional Overview** The SNMP framework consists of three parts: • An SNMP manager—The system used to control and monitor the activities of network devices using SNMP. • An SNMP agent—The software component within the managed device that maintains the data for the device and reports these data, as needed, to managing systems. Cisco NX-OS supports the agent and MIB. To enable the SNMP agent, you must define the relationship between the manager and the agent. • A managed information base (MIB)—The collection of managed objects on the SNMP agent. SNMP is defined in RFCs 3411 to 3418. Cisco NX-OS supports SNMPv1, SNMPv2c, and SNMPv3. Both SNMPv1 and SNMPv2c use a community-based form of security. Cisco NX-OS supports SNMP over IPv6. Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x (2010), at 10-2.	37.2.3 SNMP Versions Arista switches support the following SNMP versions: • **SNMPv1**: The Simple Network Management Protocol, defined in RFC 1157. Security is based on community strings. • **SNMPv2c**: Community-string based Administrative Framework for SNMPv2, defined in RFC 1901 RFC 1905, and RFC 1906. SNMPv2c uses the community-based security model of SNMPv1. • **SNMPv3**: Version 3 is an interoperable standards-based protocol defined in RFCs 2273 to 2275. SNMPv3 provides secure access to devices by authenticating and encrypting packets. The security features provided in SNMPv3 are as follows: — *Message integrity*: Ensures packets are not tampered with in transit. — *Authentication*: Determines the message is received from a valid source. — *Encryption*: Scrambling packet contents to prevent an unauthorized source from learning it. Both SNMPv1 and SNMPv2c use a community-based form of security. The community of managers able to access the agent MIB is controlled by a password. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 349. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1891;Arista User Manual v. 4.12.3 (7/17/13), at 1654; Arista User Manual, v. 4.11.1 (1/11/13), at 1341; Arista User Manual v. 4.10.3 (10/22/12), at 1107; Arista User Manual v. 4.9.3.2 (5/3/12), at 863; Arista User Manual v. 4.8.2 (11/18/11), at 675; Arista User Manual v. 4.7.3 (7/18/11), at 531.

Cisco NX-OS 4.0 Effective date of registration: 11/13/2014	Cisco NX-OS supports SNMPv1, SNMPv2c and SNMPv3. Both SNMPv1 and SNMPv2c use a community-based form of security. Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.0 (2008), at 10-2.	37.2.3 SNMP Versions Arista switches support the following SNMP versions: • **SNMPv1**: The Simple Network Management Protocol, defined in RFC 1157. Security is based on community strings. • **SNMPv2c**: Community-string based Administrative Framework for SNMPv2, defined in RFC 1901 RFC 1905, and RFC 1906. SNMPv2c uses the community-based security model of SNMPv1. • **SNMPv3**: Version 3 is an interoperable standards-based protocol defined in RFCs 2273 to 2275. SNMPv3 provides secure access to devices by authenticating and encrypting packets. The security features provided in SNMPv3 are as follows: — *Message integrity*: Ensures packets are not tampered with in transit. — *Authentication*: Determines the message is received from a valid source. — *Encryption*: Scrambling packet contents to prevent an unauthorized source from learning it. Both SNMPv1 and SNMPv2c use a community-based form of security. The community of managers able to access the agent MIB is controlled by a password. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 349. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1891;Arista User Manual v. 4.12.3 (7/17/13), at 1654; Arista User Manual, v. 4.11.1 (1/11/13), at 1341; Arista User Manual v. 4.10.3 (10/22/12), at 1107; Arista User Manual v. 4.9.3.2 (5/3/12), at 863; Arista User Manual v. 4.8.2 (11/18/11), at 675; Arista User Manual v. 4.7.3 (7/18/11), at 531.

Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	**SNMPv3** SNMPv3 provides secure access to devices by a combination of authenticating and encrypting frames over the network. The security features provided in SNMPv3 are as follows: • Message integrity—Ensures that a packet has not been tampered with while it was in-transit. • Authentication—Determines that the message is from a valid source. • Encryption—Scrambles the packet contents to prevent it from being seen by unauthorized sources. SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet. This section includes the following topics: • Security Models and Levels for SNMPv1, v2, v3, page 11-4 • User-Based Security Model, page 11-5 • CLI and SNMP User Synchronization, page 11-5 Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 11-3.	37.2.3 SNMP Versions Arista switches support the following SNMP versions: • **SNMPv1**: The Simple Network Management Protocol, defined in RFC 1157. Security is based on community strings. • **SNMPv2c**: Community-string based Administrative Framework for SNMPv2, defined in RFC 1901, RFC 1905, and RFC 1906. SNMPv2c uses the community-based security model of SNMPv1. • **SNMPv3**: Version 3 is an interoperable standards-based protocol defined in RFCs 2273 to 2275. SNMPv3 provides secure access to devices by authenticating and encrypting packets. The security features provided in SNMPv3 are as follows: — *Message integrity*: Ensures packets are not tampered with in transit. — *Authentication*: Determines the message is received from a valid source. — *Encryption*: Scrambling packet contents to prevent an unauthorized source from learning it. Both SNMPv1 and SNMPv2c use a community-based form of security. The community of managers able to access the agent MIB is controlled by a password. SNMPv2c support includes a bulk retrieval mechanism and more detailed error message reporting. The bulk retrieval mechanism supports the retrieval of tables and large quantities of information, minimizing the number of round-trips required. SNMPv2c error handling includes expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. SNMPv2c error return codes report error type. SNMPv3 is a security model which defines an authentication strategy that is configured for a user and the group in which the user resides. A security level is the permitted level of security within the model. A combination of a security model and a security level determines the security mechanism employed to handle an SNMP packet. Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 349. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1891;Arista User Manual v. 4.12.3 (7/17/13), at 1654; Arista User Manual, v. 4.11.1 (1/11/13), at 1341; Arista User Manual v. 4.10.3 (10/22/12), at 1107-08; Arista User Manual v. 4.9.3.2 (5/3/12), at 863; Arista User Manual v. 4.7.3 (7/18/11), at 531.

Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	**SNMPv3** SNMPv3 provides secure access to devices by a combination of authenticating and encrypting frames over the network. The security features provided in SNMPv3 are as follows: • Message integrity—Ensures that a packet has not been tampered with while it was in-transit. • Authentication—Determines that the message is from a valid source. • Encryption—Scrambles the packet contents to prevent it from being seen by unauthorized sources. SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet. Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x (2010), at 10-2.	37.2.3 SNMP Versions Arista switches support the following SNMP versions: • **SNMPv1**: The Simple Network Management Protocol, defined in RFC 1157. Security is based on community strings. • **SNMPv2c**: Community-string based Administrative Framework for SNMPv2, defined in RFC 1901, RFC 1905, and RFC 1906. SNMPv2c uses the community-based security model of SNMPv1. • **SNMPv3**: Version 3 is an interoperable standards-based protocol defined in RFCs 2273 to 2275. SNMPv3 provides secure access to devices by authenticating and encrypting packets. The security features provided in SNMPv3 are as follows: — *Message integrity*: Ensures packets are not tampered with in transit. — *Authentication*: Determines the message is received from a valid source. — *Encryption*: Scrambling packet contents to prevent an unauthorized source from learning it. Both SNMPv1 and SNMPv2c use a community-based form of security. The community of managers able to access the agent MIB is controlled by a password. SNMPv2c support includes a bulk retrieval mechanism and more detailed error message reporting. The bulk retrieval mechanism supports the retrieval of tables and large quantities of information, minimizing the number of round-trips required. SNMPv2c error handling includes expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. SNMPv2c error return codes report error type. SNMPv3 is a security model which defines an authentication strategy that is configured for a user and the group in which the user resides. A security level is the permitted level of security within the model. A combination of a security model and a security level determines the security mechanism employed to handle an SNMP packet. Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 349. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1891;Arista User Manual v. 4.12.3 (7/17/13), at 1654; Arista User Manual, v. 4.11.1 (1/11/13), at 1341; Arista User Manual v. 4.10.3 (10/22/12), at 1107-08; Arista User Manual v. 4.9.3.2 (5/3/12), at 863; Arista User Manual v. 4.7.3 (7/18/11), at 531.

Cisco NX-OS 4.0 Effective date of registration: 11/13/2014	**SNMPv3** SNMPv3 provides secure access to devices by a combination of authenticating and encrypting frames over the network. The security features provided in SNMPv3 are as follows: • Message integrity—Ensures that a packet has not been tampered with while it was in-transit. • Authentication—Determines that the message is from a valid source. • Encryption—Scrambles the packet contents to prevent it from being seen by unauthorized sources. SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet. Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.0 (2008), at 7-2.	37.2.3 SNMP Versions Arista switches support the following SNMP versions: • **SNMPv1**: The Simple Network Management Protocol, defined in RFC 1157. Security is based on community strings. • **SNMPv2c**: Community-string based Administrative Framework for SNMPv2, defined in RFC 1901, RFC 1905, and RFC 1906. SNMPv2c uses the community-based security model of SNMPv1. • **SNMPv3**: Version 3 is an interoperable standards-based protocol defined in RFCs 2273 to 2275. SNMPv3 provides secure access to devices by authenticating and encrypting packets. The security features provided in SNMPv3 are as follows: — *Message integrity*: Ensures packets are not tampered with in transit. — *Authentication*: Determines the message is received from a valid source. — *Encryption*: Scrambling packet contents to prevent an unauthorized source from learning it. Both SNMPv1 and SNMPv2c use a community-based form of security. The community of managers able to access the agent MIB is controlled by a password. SNMPv2c support includes a bulk retrieval mechanism and more detailed error message reporting. The bulk retrieval mechanism supports the retrieval of tables and large quantities of information, minimizing the number of round-trips required. SNMPv2c error handling includes expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. SNMPv2c error return codes report error type. SNMPv3 is a security model which defines an authentication strategy that is configured for a user and the group in which the user resides. A security level is the permitted level of security within the model. A combination of a security model and a security level determines the security mechanism employed to handle an SNMP packet. Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 349. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1891;Arista User Manual v. 4.12.3 (7/17/13), at 1654; Arista User Manual, v. 4.11.1 (1/11/13), at 1341; Arista User Manual v. 4.10.3 (10/22/12), at 1107-08; Arista User Manual v. 4.9.3.2 (5/3/12), at 863; Arista User Manual v. 4.7.3 (7/18/11), at 531.
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	SNMPv3 uses contexts to distinguish between these multiple instances. An SNMP context is a collection of management information that you can access through the SNMP agent. A device can support multiple contexts for different logical network entities. An SNMP context allows the SNMP manager to access one of the multiple instances of a MIB module supported on the device for the different logical network entities. Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 11-3.	An SNMP context is a collection of management information items accessible by an SNMP entity. Each item of may exist in multiple contexts. Each SNMP entity can access multiple contexts. A context is identified by the EngineID of the hosting device and a context name. Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 1994. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1684; Arista User Manual, v. 4.11.1 (1/11/13), at 1369; Arista User Manual v. 4.10.3 (10/22/12), at 1136; Arista User Manual v. 4.9.3.2 (5/3/12), at 892; Arista User Manual v. 4.8.2 (11/18/11), at 699; Arista User Manual v. 4.7.3 (7/18/11), at 555.

Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	
	Step 2 `vlan vlan`
	Example:
	`switch(config)# vlan 901`
	`switch(config-vlan)#`
	Enters VLAN configuration mode for the VLAN specified.
	
	Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 16-18.
		
		Example
		• This command creates VLAN 49 and enters VLAN configuration mode for the new VLAN:
		`switch(config)#vlan 49`
		`switch(config-vlan-49)#`
		
		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 803.
		
		See also Arista User Manual v. 4.12.3 (7/17/13), at 650; Arista User Manual, v. 4.11.1 (1/11/13), at 502; Arista User Manual v. 4.10.3 (10/22/12), at 420; Arista User Manual v. 4.9.3.2 (5/3/12), at 359.

Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	To permit the discovery of non-Cisco devices, the switch also supports the *Link Layer Discovery Protocol (LLDP)*, a vendor-neutral device discovery protocol that is defined in the IEEE 802.1ab standard. LLDP allows network devices to advertise information about themselves to other devices on the network. This protocol runs over the data-link layer, which allows two systems running different network layer protocols to learn about each other. Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 18-2.	Link Layer Discovery Protocol (LLDP) allows Ethernet network devices to advertise details about themselves, such as device configuration, capabilities and identification, to directly connected devices on the network that are also using LLDP. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 572. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 447; Arista User Manual, v. 4.11.1 (1/11/13), at 365.
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	**Guidelines and Limitations** LLDP has the following configuration guidelines and limitations: • LLDP must be enabled on the device before you can enable or disable it on any interfaces. • LLDP is supported only on physical interfaces. • LLDP can discover up to one device per port. • LLDP can discover Linux servers, provided they are not using a converged network adapter (CNA). LLDP cannot discover other types of servers. • DCBXP incompatibility messages might appear when you change the network QoS policy, if a physical loopback connection is in the device. The incompatibility exists for only a short time and then clears. • DCBXP is not supported for the Cisco Nexus 2000 Series Fabric Extender. • Beginning with Cisco NX-OS Release 5.2, LLDP is supported for the Cisco Nexus 2000 Series Fabric Extender. LLDP packets can now be sent and received through the Fabric Extender ports for neighbor discovery. – All LLDP configuration on Fabric Extender ports occurs on the supervisor. LLDP configuration and show commands are not visible on the Fabric Extender console. – LLDP is not supported for a Fabric Extender-virtual port channel (vPC) connection. Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 18-2.	12.2.4 Guidelines and Limitations LLDP has the following configuration guidelines and limitations: • LLDP must be enabled on the device before you can enable or disable it on any interface. • LLDP is supported only on physical interfaces. • LLDP can discover up to one device per port. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 576. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 448; Arista User Manual, v. 4.11.1 (1/11/13), at 366.

Cisco NX-OS 6.2

Effective date of registration: 11/13/2014

Enabling or Disabling LLDP on an Interface

After you globally enable LLDP, it is enabled on all supported interfaces by default. However, you can enable or disable LLDP on individual interfaces or selectively configure an interface to only send or only receive LLDP packets.

Note If the interface is configured as a tunnel port, LLDP is disabled automatically.

BEFORE YOU BEGIN

Make sure that you are in the correct VDC. To switch VDCs, use the **switchto vdc** command.

Make sure that you have globally enabled LLDP on the device.

SUMMARY STEPS

1. **config t**
2. **interface ethernet** *slot/port*
3. **[no] lldp transmit**
4. **[no] lldp receive**
5. (Optional) **show lldp interface ethernet** *slot/port*
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`switch# config t`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface ethernet** *slot/port*
	
	Example:
	`switch(config)# interface ethernet 7/1`
	`switch(config-if)`
		Specifies the interface on which you are enabling LLDP and enters the interface configuration mode.

Step 3	**[no] lldp transmit** **Example:** `switch(config-if)# lldp transmit`	Enables or disables the transmission of LLDP packets on an interface. After you globally enable LLDP, it is enabled on all supported interfaces by default.
Step 4	**[no] lldp receive** **Example:** `switch(config-if)# lldp receive`	Enables or disables the reception of LLDP packets on an interface. After you globally enable LLDP, it is enabled on all supported interfaces by default.

Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 18-6.

12.3.2 Enabling LLDP on an Interface

After you globally enable LLDP, it is enabled on all supported interfaces by default. However, by using the **lldp transmit** and **lldp receive** commands, you can enable or disable LLDP on individual interfaces or selectively configure an interface to only send or only receive LLDP packets.

Examples

- These commands enable Ethernet port 3/1 to transmit LLDP packets.

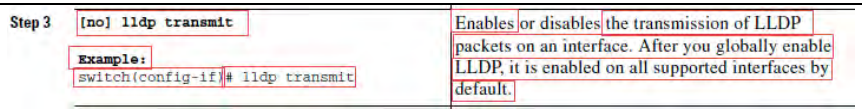
```
switch(config)# interface ethernet 3/1
switch(config-if-Et3/1)# lldp transmit
switch(config-if-Et3/1)#
```

- These commands enable Ethernet port 3/1 to receive LLDP packets.

```
switch(config)# interface ethernet 3/1
switch(config-if-Et3/1)# lldp receive
switch(config-if-Et3/1)#
```

Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 577.

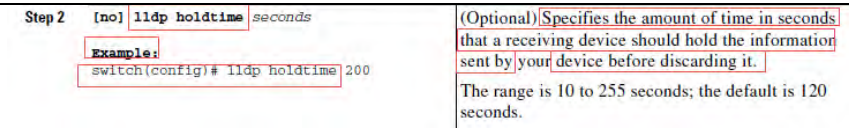
See also Arista User Manual v. 4.12.3 (7/17/13), at 449; Arista User Manual, v. 4.11.1 (1/11/13), at 367.

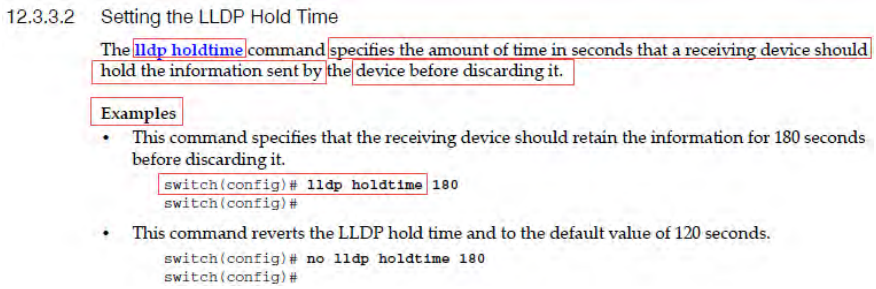
Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	
	Step 3 [no] lldp transmit
	Example:
	switch(config-if)# lldp transmit
	Enables or disables the transmission of LLDP packets on an interface. After you globally enable LLDP, it is enabled on all supported interfaces by default.
	
	Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 18-6.
		lldp transmit
		
		The **lldp transmit** command enables the transmission of LLDP packets on an interface. After you globally enable LLDP, it is enabled on all supported interfaces by default.
		
		Platform all
		Command Mode Interface-Ethernet configuration
		Interface-Management configuration
		
		Command Syntax
		`lldp transmit`
		`no lldp transmit`
		`default lldp transmit`
		
		Examples
		• These commands enable the transmission of LLDP packets on a specific interface.
		`switch(config)#interface ethernet 4/1`
		`switch(config-if-Et4/1)#lldp transmit`
		`switch(config-if-Et4/1)#`
		• These commands disable the transmission of LLDP packets on a specific interface.
		`switch(config)#interface ethernet 4/1`
		`switch(config-if-Et4/1)#no lldp transmit`
		`switch(config-if-Et4/1)#`
		
		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 593.
		
		See also Arista User Manual v. 4.12.3 (7/17/13), at 466; Arista User Manual, v. 4.11.1 (1/11/13), at 384.

Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	Step 4 `[no] lldp receive` — Enables or disables the reception of LLDP packets on an interface. After you globally enable LLDP, it is enabled on all supported interfaces by default.
	Example: `switch(config-if)# lldp receive`
	
	Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 18-6.
		lldp receive
		
		The lldp receive command enables the reception of LLDP packets on an interface. After you globally enable LLDP, it is enabled on all supported interfaces by default. The no form of the is command disables the reception of LLDP packets on an interface.
		
		Platform: all
		Command Mode: Interface-Ethernet configuration
		Interface-Management configuration
		
		Command Syntax
		`lldp receive`
		`no lldp receive`
		`default lldp receive`
		
		Examples
		• These commands enables the reception of LLDP packets on a specific interface.
		`switch(config)#interface ethernet 4/1`
		`switch(config-if-Et4/1)#lldp receive`
		`switch(config-if-Et4/1)#`
		• These commands disables LLDP the reception of LLDP packets on a specific interface.
		`switch(config)#interface ethernet 4/1`
		`switch(config-if-Et4/1)# no lldp receive`
		`switch(config-if-Et4/1)#`
		
		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 588.
		
		See also Arista User Manual v. 4.12.3 (7/17/13), at 461; Arista User Manual, v. 4.11.1 (1/11/13), at 379.

Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	**Configuring Optional LLDP Parameters** You can configure the frequency of LLDP updates, the amount of time for a receiving device to hold the information before discarding it, and the initialization delay time. You can also select the TLVs to include in LLDP packets. Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 18-7.	12.3.3 Optional LLDP Parameters You can globally configure the frequency of LLDP updates, the amount of time for a receiving device to hold the information before discarding it, and the initialization delay time. You can also select the TLVs to include in LLDP packets. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 577. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 449; Arista User Manual, v. 4.11.1 (1/11/13), at 367.

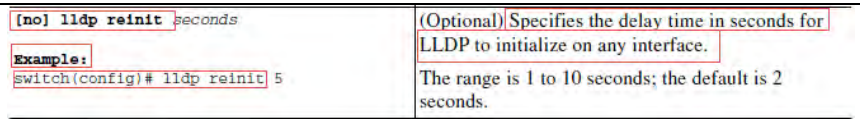
<table>
<tr>
<td>Cisco NX-OS 6.2

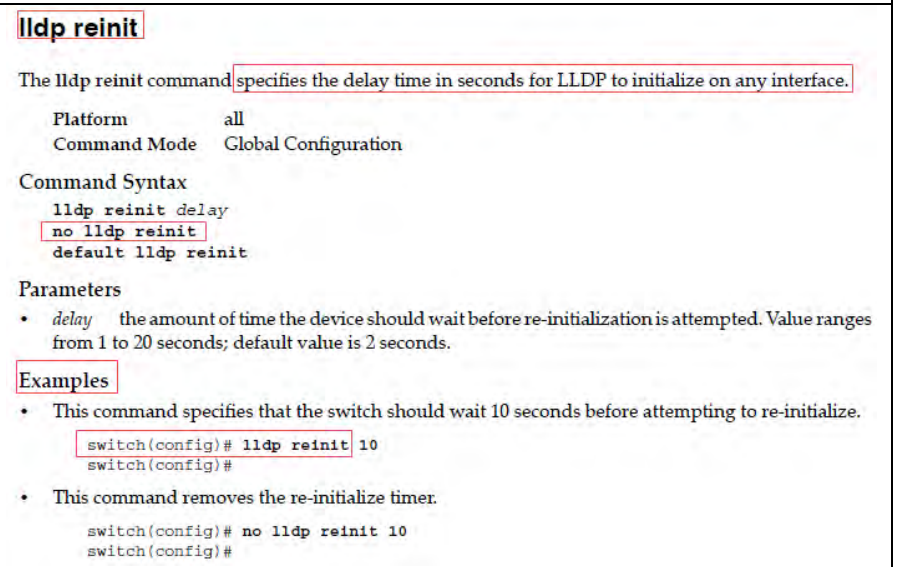
Effective date of registration: 11/13/2014</td>
<td>


Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 18-8.
</td>
<td>


Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 578.

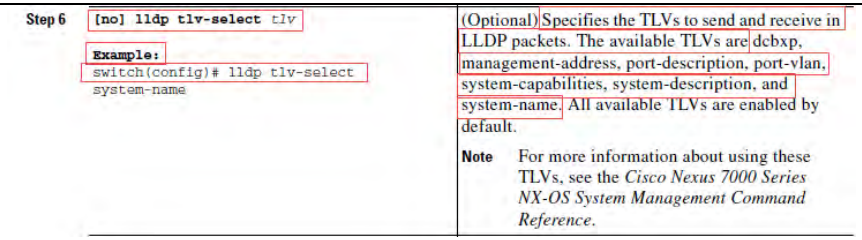
See also Arista User Manual v. 4.12.3 (7/17/13), at 450; Arista User Manual, v. 4.11.1 (1/11/13), at 368.
</td>
</tr>
<tr>
<td>Cisco NX-OS 6.2

Effective date of registration: 11/13/2014</td>
<td>


Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 18-8.
</td>
<td>


Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 589.

See also Arista User Manual v. 4.13.6F (4/14/2014), at 318; Arista User Manual v. 4.12.3 (7/17/13), at 262; Arista User Manual, v. 4.11.1 (1/11/13), at 208.
</td>
</tr>
</table>

Cisco NX-OS 6.2
 	
Effective date of registration: 11/13/2014
	
	Step 6 `[no] lldp tlv-select tlv`
	Example:
	`switch(config)# lldp tlv-select system-name`
	(Optional) Specifies the TLVs to send and receive in LLDP packets. The available TLVs are dcbxp, management-address, port-description, port-vlan, system-capabilities, system-description, and system-name. All available TLVs are enabled by default.
	Note For more information about using these TLVs, see the *Cisco Nexus 7000 Series NX-OS System Management Command Reference*.
	
	Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 18-8.
		lldp tlv-select
		
		The **lldp tlv-select** command allows the user to specify the TLVs to send and receive in LLDP packets. The available TLVs are management-address, port-description, port-vlan, system-capabilities, system-description, and system-name.
		
		Platform all
		Command Mode Global Configuration
		
		Command Syntax
		`lldp tlv-select TLV_NAME`
		`no lldp tlv-select TLV_NAME`
		`default lldp tlv-select TLV_NAME`
		
		Parameters
		• *TLV_NAME* the TLV specifies the information to be sent or received in the LLDP packet: Options include:
		— **link-aggregation** specifies the link aggregation TLV.
		— **management-address** specifies the management address TLV.
		— **max-frame-size** specifies the Frame size TLV.
		— **port-description** specifies the port description TLV.
		— **port-vlan** specifies the port VLAN ID TLV.
		— **system-capabilities** specifies the system capabilities TLV.
		— **system-description** specifies the system description TLV.
		— **system-name** specifies the system name TLV.
		
		Example
		• This command enables the system description TLV:
		`switch(config)# lldp tlv-select system-description`
		`switch(config)#`
		• This command disables the system description TLV:
		`switch(config)# no lldp tlv-select system-description`
		`switch(config)#`
		• This command enables the max-frame-size TLV:
		`switch(config)# lldp tlv-select max-frame-size`
		`switch(config)#`
		• This command disables the max-frame-size TLV:
		`switch(config)# no lldp tlv-select max-frame-size`
		`switch(config)#`
		
		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 592.
		
		See also Arista User Manual v. 4.12.3 (7/17/13), at 465; Arista User Manual, v. 4.11.1 (1/11/13), at 383.

Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	**show lldp traffic** — Displays the LLDP counters, including the number of LLDP packets sent and received by the device, the number of discarded packets, and the number of unrecognized TLVs. Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 18-9.	12.3.5.4 Viewing LLDP Traffic The show lldp traffic command displays the LLDP counters, including the number of packets sent and received, and the number of packets discarded by the switch. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 581. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 454; Arista User Manual, v. 4.11.1 (1/11/13), at 372.